PCT/JP00/09129

22.12.00

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

JP00/9129

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

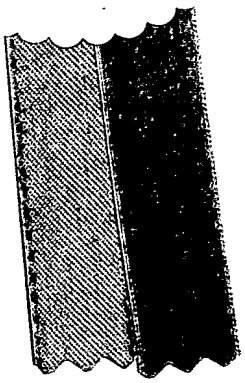
出願年月日
Date of Application: ２０００年　１月１４日

出願番号
Application Number: 特願２０００－００５１６１

出願人
Applicant (s): 三菱電機株式会社

4

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)



２００１年　２月　９日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３００５３９５

【書類名】　特許願

【整理番号】　522196JP01

【提出日】　平成12年 1月14日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/06

【発明者】

【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

【氏名】　反町　亨

【発明者】

【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

【氏名】　時田　俊雄

【特許出願人】

【識別番号】　000006013

【氏名又は名称】　三菱電機株式会社

【代理人】

【識別番号】　100099461

【弁理士】

【氏名又は名称】　溝井　章司

【選任した代理人】

【識別番号】　100111497

【弁理士】

【氏名又は名称】　波田　啓子

【選任した代理人】

【識別番号】　100111800

【弁理士】

【氏名又は名称】　竹内　三明

【手数料の表示】

【予納台帳番号】　056177

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9903016

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化装置及び暗号化方法及び復号装置及び復号方法

【特許請求の範囲】

【請求項１】　１つ以上のブロックデータからなる第１の処理データと、１つ以上のブロックデータからなる第２の処理データとの暗号化処理をする暗号化装置において、

暗号化処理の状態を記憶するメモリを備え、

第１の処理データの全ブロックデータの暗号化処理が完了する前に第２の処理データの最初のブロックデータの暗号化処理を開始するとともに、第２の処理データの最初のブロックデータの暗号化処理を開始する場合に第１の処理データの暗号化処理の状態を上記メモリに記憶させ、第１の処理データの暗号化処理を再開する場合に暗号化装置の暗号化処理の状態をメモリに記憶した第１の処理データの暗号化処理の状態に復帰させてから第１の処理データの暗号化処理を再開することを特徴とする暗号化装置。

【請求項２】　上記暗号化装置は、第２の処理データの全ブロックデータの暗号処理の完了する前に第１の処理データの暗号化処理を再開するとともに、上記メモリは、第１の処理データの暗号化処理を再開する場合に第２の処理データの暗号化処理状態を記憶し、第２の処理データの暗号化処理を再開する場合は、暗号化装置の暗号化処理の状態をメモリに記憶した第２の処理データの暗号化処理の状態に復帰させてから第２の処理データの暗号化処理を再開することを特徴とする請求項１記載の暗号化装置。

【請求項３】　上記第１の処理データは、第１の平文であり、上記第２の処理データは、第２の平文であることを特徴とする請求項１記載の暗号化装置。

【請求項４】　上記暗号化装置は、割り込みにより第２の処理データの最初のブロックデータの暗号化処理を開始することを特徴とする請求項１記載の暗号化装置。

【請求項５】　平文Ｍを構成する平文ブロックデータM_i（ｉ＝１，２，３，・・・）と平文Ｎを構成する平文ブロックデータN_j（ｊ＝１，２，３，・・・）とを暗号化する暗号化装置において、

平文Mの暗号化処理中に平文Nの暗号化要求を平文Mの暗号化処理完了前に受け付けるメカニズムと、

暗号化処理を行い中間ブロックデータT_i又は暗号文ブロックデータC_iを出力する暗号化モジュールと、

暗号化モジュールから出力された中間ブロックデータT_i又は暗号文ブロックデータC_iをフィードバックラインを介し暗号化モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記平文Nの暗号化要求を受け付け、平文Nのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されない場合、フィードバックされるブロックデータを記憶するメモリと、

平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化される場合は、上記フィードバックループのフィードバックラインによりフィードバックされるブロックデータを選択してフィードバックループに供給し、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されず、平文Nのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリに記憶されたブロックデータを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする暗号化装置。

【請求項６】　上記メモリは、

複数の平文に対応した複数のレジスタと、

暗号化処理をする平文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする請求項５記載の暗号化装置。

【請求項７】　暗号化モジュールを用いて第１の平文Mの平文ブロックデータM_i（ｉ＝１，２，３，・・・）を暗号化する工程と、

上記平文ブロックデータM_iを暗号化している途中で又は平文ブロックデータM_iを暗号化した後に、第１の平文Mの平文ブロックデータM_{i+1}の暗号化に用いられる中間ブロックデータT_i又は暗号文ブロックデータC_iをメモリに記憶

する工程と、

上記平文ブロックデータM_{i+1}の暗号化に用いられるブロックデータをメモリに記憶した後に、第２の平文Ｎの少なくとも１つの平文ブロックデータを暗号化する工程と、

上記第２の平文Ｎの少なくとも１つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータM_{i+1}の暗号化に用いられるブロックデータを入力し、暗号化モジュールを用いて第１の平文Ｍの平文ブロックデータM_{i+1}を暗号化する工程と

を備えたことを特徴とする暗号化方法。

【請求項８】　１つ以上の平文ブロックデータからなる平文を暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、

平文ブロックデータを暗号化したときに生成した中間ブロックデータT_i又は暗号文ブロックデータC_iをフィードバックする第１のフィードバックループを有し、平文ブロックデータを入力し、第１のフィードバックループによりブロックデータをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部と

を備えたことを特徴とする暗号化装置。

【請求項９】　上記暗号化部と認証子生成部とは、１つの暗号化モジュールと、１つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理

と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタと

を備えたことを特徴とする請求項８記載の暗号化装置。

【請求項１０】　１つ以上の平文ブロックデータからなる平文を暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

平文ブロックデータを暗号化したときに生成した中間ブロックデータT_i又は暗号文ブロックデータC_iをフィードバックする第１のフィードバック工程を有し、平文ブロックデータを入力し、第１のフィードバックループによりブロックデータをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程と

を備えたことを特徴とする暗号化方法。

【請求項１１】　１つ以上のブロックデータからなる第１の処理データと、１つ以上のブロックデータからなる第２の処理データとの復号処理をする復号装置において、

復号処理の状態を記憶するメモリを備え、

第１の処理データの全ブロックデータの復号処理が完了する前に第２の処理データの最初のブロックデータの復号処理を開始するとともに、第２の処理データの最初のブロックデータの復号処理を開始する場合に第１の処理データの復号処理の状態を上記メモリに記憶させ、第１の処理データの復号処理を再開する場合に復号装置の復号処理の状態をメモリに記憶した第１の処理データの復号処理の状態に復帰させてから第１の処理データの復号処理を再開することを特徴とする復号装置。

【請求項１２】　上記復号装置は、第２の処理データの全ブロックデータの

復号処理の完了する前に第１の処理データの復号処理を再開するとともに、上記メモリは、第１の処理データの復号処理を再開する場合に第２の処理データの復号処理状態を記憶し、第２の処理データの復号処理を再開する場合は、復号装置の復号処理の状態をメモリに記憶した第２の処理データの復号処理の状態に復帰させてから第２の処理データの復号処理を再開することを特徴とする請求項１１記載の復号装置。

【請求項１３】　上記第１の処理データは、第１の暗号文であり、上記第２の処理データは、第２の暗号文であることを特徴とする請求項１１記載の復号装置。

【請求項１４】　上記復号装置は、割り込みにより第２の処理データの最初のブロックデータの復号処理を開始することを特徴とする請求項１１記載の復号装置。

【請求項１５】　暗号文Ｃを構成する暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）と暗号文Ｎを構成する暗号文ブロックデータN_j（ｊ＝１，２，３，・・・）とを復号する復号装置において、

暗号文Ｃの復号処理中に暗号文Ｎの復号要求を任意の時点で受け付けるメカニズムと、

復号処理を行い中間ブロックデータT_i又は平文ブロックデータM_iを出力する復号モジュールと、

復号モジュールから出力された中間ブロックデータT_i又は平文ブロックデータM_iをフィードバックラインを介し復号モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Ｎの復号要求を受け付け、暗号文Ｎのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されない場合、フィードバックされるブロックデータを記憶するメモリと、

暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号される場合は、上記フィードバックループのフィードバックラインによりフィード

バックされるブロックデータを選択してフィードバックループに供給し、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されず、暗号文Ｎのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶されたブロックデータを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする復号装置。

【請求項１６】　上記メモリは、

複数の暗号文に対応した複数のレジスタと、

復号処理をする暗号文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする請求項１１記載の復号装置。

【請求項１７】　復号モジュールを用いて第１の暗号文Ｃの暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）を復号する工程と、

上記暗号文ブロックデータC_iを復号している途中で又は暗号文ブロックデータC_iを復号した後に、第１の暗号文Ｃの暗号文ブロックデータC_{i+1}の復号に用いられる中間ブロックデータT_i又は平文ブロックデータM_iをメモリに記憶する工程と、

上記暗号文ブロックデータC_{i+1}の復号に用いられるブロックデータをメモリに記憶した後に、第２の暗号文Ｎの少なくとも１つの暗号文ブロックデータを復号する工程と、

上記第２の暗号文Ｎの少なくとも１つの暗号文ブロックデータを復号した後に、メモリに記憶された、暗号文ブロックデータC_{i+1}の復号に用いられるブロックデータを入力し、復号モジュールを用いて第１の暗号文Ｃの暗号文ブロックデータC_{i+1}を復号する工程と

を備えたことを特徴とする復号方法。

【請求項１８】　１つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

暗号文ブロックデータを復号したときに生成した中間ブロックデータT_i又は平文ブロックデータM_iをフィードバックする第１のフィードバックループを有

し、暗号文ブロックデータを入力し、第１のフィードバックループによりブロックデータをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と

を備えたことを特徴とする復号装置。

【請求項１９】　上記復号部と認証子生成部とは、１つの復号モジュールと、１つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

復号処理と認証生成処理とを交互に実行するために、メモリから復号処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクタと

を備えたことを特徴とする請求項１８記載の復号装置。

【請求項２０】　１つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

暗号文ブロックデータを復号したときに生成した中間ブロックデータT_i 又は平文ブロックデータM_i をフィードバックする第１のフィードバック工程を有し、暗号文ブロックデータを入力し、第１のフィードバックループによりブロックデータをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、復号工程に入力される暗号文のブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認す

るための認証子を生成する認証子生成工程と

を備えたことを特徴とする復号方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、暗号化復号装置及び暗号化復号方法に関するものである。特に、データの暗号化復号の最中に他のデータの暗号化復号ができる発明に関するものである。

【０００２】

【従来の技術】

図３２は、Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ　Ｍｏｄｅ（以下、ＣＢＣモードという）による暗号化装置を示す図である。

図３２に示すＣＢＣモードでの暗号方法は、６４ビットの平文ブロックデータM_iをブロック単位で入力して、暗号鍵Ｋを用いた暗号化モジュール５１により暗号化し、更に、この暗号化された暗号文ブロックデータC_iと次の平文ブロックデータM_{i+1}との排他的論理和を演算し、排他的論理和の演算結果を次の暗号化の入力として、暗号鍵Ｋを用いた暗号化モジュール５１に供給することにより暗号化する方法である。そして、この処理を繰り返して次々と連鎖させることにより、平文Ｍ全体を暗号文Ｃに暗号化するものである。

【０００３】

図３３は、ＣＢＣモードを用いた復号装置を示す図である。

図３３に示す復号装置は、図３２に示す暗号化装置により暗号化された暗号文を復号する装置である。暗号文ブロックデータC_1が暗号鍵Ｋを用いた復号モジュール７１に入力され、イニシャルバリューＩＶとの排他的論理和が計算され、平文ブロックデータM_1が復号される。暗号文ブロックデータC_2が入力された場合には、暗号鍵Ｋを用いた復号モジュール７１で復号され、先に入力され、レジスタ１１１に保存された暗号文ブロックデータC_1との排他的論理和がとられ、平文ブロックデータM_2を復号する。

【０００４】

平文ブロックデータをM_i（ｉ＝１，２，・・・，ｎ）、暗号文ブロックデータC_i（ｉ＝１，２，・・・，ｎ）とし、暗号鍵Ｋを用いた暗号化処理をE_K、暗号鍵Ｋを用いた復号処理をD_Kとすると、ＣＢＣモードは次式で表される。

$C_1 = E_K\ (M_1\ EXR\ IV)$

$C_i = E_K\ (M_i\ EXR\ C_{i-1})$（ｉ＝２，３，・・・，ｎ）

$M_1 = D_K\ (C_1)\ EXR\ IV$

$M_i = D_K\ (C_i)\ EXR\ C_{i-1}$（ｉ＝２，３，・・・，ｎ）

ここで、ＥＸＲは排他的論理和演算である。また、ＩＶ（Ｉｎｔｉａｌ　Ｖａｌｕｅ）は初期値であり、最初の暗号化と復号の際に用いられる。イニシャルバリューＩＶは、暗号化側と復号側で同一の値を用いる。

【０００５】

図３４は、Ｏｕｔｐｕｔ　Ｆｅｅｄｂａｃｋ　Ｍｏｄｅ（以下、ＯＦＢモードという）の暗号化装置を示す図である。

図３５は、ＯＦＢモードの復号装置を示す図である。

図３６は、Ｃｉｐｈｅｒ　Ｆｅｅｄｂａｃｋ　Ｍｏｄｅ（以下、ＣＦＢモードという）の暗号化装置を示す図である。

図３７は、ＣＦＢモードの復号装置を示す図である。

【０００６】

図３８は、ＣＢＣモードの暗号化装置を用いて平文Ｍと平文Ｎを暗号化する手順を示す図である。

ここでは、平文Ｍが平文ブロックデータM_1，平文ブロックデータM_2，平文ブロックデータM_3から構成されており、平文Ｎが平文ブロックデータN_1のみで構成されている場合を説明する。

平文ブロックデータM_1の暗号化がスタートすると、暗号文ブロックデータC_1が出力されるとともに、暗号文ブロックデータC_1は、平文ブロックデータM_2の暗号化に用いられる。このように、暗号文ブロックデータC_iは、平文ブロックデータM_{i+1}の暗号化にフィードバックされて連鎖処理が行われる。従って、平文ブロックデータM_1から平文ブロックデータM_3までの暗号化が終わらなければ、平文ブロックデータN_1の暗号化を行うことができない。

【０００７】

図３９は、図３８と同様に、ＣＢＣモードで暗号化を行う場合を示している。

図３９の場合は、平文ブロックデータM_1、平文ブロックデータM_2、平文ブロックデータM_3の各データが準備されるのに時間がかかってしまう場合を示している。一方、暗号化処理は、次の平文ブロックデータM_{i+1}が準備できる前に終了しており、アイドル時間（例えば、Ｔ１～Ｔ２、Ｔ３～Ｔ４の時間）が発生してしまう場合を示している。このように、アイドル時間が発生する場合でも、暗号文ブロックデータC_iが次の平文ブロックデータM_{i+1}にフィードバックされる連鎖処理を行わなければならないため、平文ブロックデータN_1の処理は平文ブロックデータM_3の処理が終了してからでなければ行えない。

【０００８】

図４０は、データの秘匿処理とデータの完全性を保証する処理を示す図である。平文Ｍは、例えば、ＯＦＢモードの暗号装置により暗号文Ｃに暗号化される。ＣＢＣモードの暗号装置により認証子Ｐが演算され、暗号文Ｃの最後に認証子Ｐが付加される。暗号化され、かつ、認証子Ｐが付加されたデータを受信した場合には、暗号文Ｃから平文ＭをＯＦＢモードの復号装置により復号するとともに、暗号文ＣからＣＢＣモードの復号装置により認証子Ｐを演算し、伝送されてきた認証子Ｐと同一か否かを比較することにより、伝送されてきたＣが改竄されていないことを確認することができる。

【０００９】

図４１は、図４０に示した秘匿処理と認証子演算処理の手順を示す図である。

平文ブロックデータM_1～平文ブロックデータM_3は、順に暗号文ブロックデータC_1～暗号文ブロックデータC_3に暗号化される。その後、暗号文ブロックデータC_1～暗号文ブロックデータC_3を順に入力して認証子Ｐが演算される。

【００１０】

【発明が解決しようとする課題】

図３１～図３７に示した各モードの暗号化装置及び復号装置は、前のブロックデータの暗号化復号されたデータをフィードバックさせて次のブロックデータの暗号化復号処理に利用しなければならないため、一旦暗号化処理又は復号処理が

スタートしてしまうと、その全体の処理が終了しない限り、他の暗号化処理又は復号処理をスタートさせることができないという課題があった。従って、先にスタートした暗号化復号処理が長時間要するものである場合には、後からスタートする暗号化復号処理が長時間待たされてしまうという課題があった。

【００１１】

また、暗号化復号されるデータが準備される時間に比べて、暗号化復号処理に要する時間が短い場合には、暗号化復号化装置にアイドル時間が発生してしまうという課題があった。

【００１２】

また、秘匿処理と完全性保証処理を行う場合には、秘匿処理を行ってから完全性保証処理を行わなければならず、処理時間がかかってしまうという課題があった。

【００１３】

この発明の好適な実施の形態によれば、あるデータの暗号化復号処理の最中に他のデータの暗号化復号処理を行える暗号化装置、復号装置及び暗号化方法及び復号方法を得ることを目的とする。

【００１４】

また、この発明の好適な実施の形態においては、優先度の高いデータの暗号化復号を優先的に行えるようにすることを目的とする。

【００１５】

また、この発明の好適な実施の形態においては、秘匿処理と完全性保証処理を並列的に高速に行えるようにすることを目的とする。

【００１６】

【課題を解決するための手段】

この発明に係る暗号化装置は、１つ以上のブロックデータからなる第１の処理データと、１つ以上のブロックデータからなる第２の処理データとの暗号化処理をする暗号化装置において、

暗号化処理の状態を記憶するメモリを備え、

第１の処理データの全ブロックデータの暗号化処理が完了する前に第２の処理

データの最初のブロックデータの暗号化処理を開始するとともに、第２の処理データの最初のブロックデータの暗号化処理を開始する場合に第１の処理データの暗号化処理の状態を上記メモリに記憶させ、第１の処理データの暗号化処理を再開する場合に暗号化装置の暗号化処理の状態をメモリに記憶した第１の処理データの暗号化処理の状態に復帰させてから第１の処理データの暗号化処理を再開することを特徴とする。

【００１７】

上記暗号化装置は、第２の処理データの全ブロックデータの暗号処理の完了する前に第１の処理データの暗号化処理を再開するとともに、上記メモリは、第１の処理データの暗号化処理を再開する場合に第２の処理データの暗号化処理状態を記憶し、第２の処理データの暗号化処理を再開する場合は、暗号化装置の暗号化処理の状態をメモリに記憶した第２の処理データの暗号化処理の状態に復帰させてから第２の処理データの暗号化処理を再開することを特徴とする。

【００１８】

上記第１の処理データは、第１の平文であり、上記第２の処理データは、第２の平文であることを特徴とする。

【００１９】

上記暗号化装置は、割り込みにより第２の処理データの最初のブロックデータの暗号化処理を開始することを特徴とする。

【００２０】

この発明に係る暗号化装置は、平文Ｍを構成する平文ブロックデータM_i（ｉ＝１，２，３，・・・）と平文Ｎを構成する平文ブロックデータN_j（ｊ＝１，２，３，・・・）とを暗号化する暗号化装置において、

平文Ｍの暗号化処理中に平文Ｎの暗号化要求を平文Ｍの暗号化処理完了前に受け付けるメカニズムと、

暗号化処理を行い中間ブロックデータT_i又は暗号文ブロックデータC_iを出力する暗号化モジュールと、

暗号化モジュールから出力された中間ブロックデータT_i又は暗号文ブロックデータC_iをフィードバックラインを介し暗号化モジュールにフィードバックす

るフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記平文Ｎの暗号化要求を受け付け、平文Ｎのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されない場合、フィードバックされるブロックデータを記憶するメモリと、

平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化される場合は、上記フィードバックループのフィードバックラインによりフィードバックされるブロックデータを選択してフィードバックループに供給し、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されず、平文Ｎのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリに記憶されたブロックデータを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする。

【００２１】

上記メモリは、

複数の平文に対応した複数のレジスタと、

暗号化処理をする平文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする。

【００２２】

この発明に係る暗号化方法は、暗号化モジュールを用いて第１の平文Ｍの平文ブロックデータM_i（ｉ＝１，２，３，・・・）を暗号化する工程と、

上記平文ブロックデータM_iを暗号化している途中で又は平文ブロックデータM_iを暗号化した後に、第１の平文Ｍの平文ブロックデータM_{i+1}の暗号化に用いられる中間ブロックデータT_i又は暗号文ブロックデータC_iをメモリに記憶する工程と、

上記平文ブロックデータM_{i+1}の暗号化に用いられるブロックデータをメモリに記憶した後に、第２の平文Ｎの少なくとも１つの平文ブロックデータを暗号化する工程と、

上記第２の平文Ｎの少なくとも１つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータM_{i+1}の暗号化に用いられるブロックデータを入力し、暗号化モジュールを用いて第１の平文Ｍの平文ブロックデータM_{i+1}を暗号化する工程と
を備えたことを特徴とする。

【００２３】

この発明に係る暗号化装置は、１つ以上の平文ブロックデータからなる平文を暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、

平文ブロックデータを暗号化したときに生成した中間ブロックデータT_i又は暗号文ブロックデータC_iをフィードバックする第１のフィードバックループを有し、平文ブロックデータを入力し、第１のフィードバックループによりブロックデータをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部と
を備えたことを特徴とする。

【００２４】

上記暗号化部と認証子生成部とは、１つの暗号化モジュールと、１つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタと

を備えたことを特徴とする。

【００２５】

この発明に係る暗号化方法は、１つ以上の平文ブロックデータからなる平文を暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

平文ブロックデータを暗号化したときに生成した中間ブロックデータT_i又は暗号文ブロックデータC_iをフィードバックする第１のフィードバック工程を有し、平文ブロックデータを入力し、第１のフィードバックループによりブロックデータをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程と

を備えたことを特徴とする。

【００２６】

この発明に係る復号装置は、１つ以上のブロックデータからなる第１の処理データと、１つ以上のブロックデータからなる第２の処理データとの復号処理をする復号装置において、

復号処理の状態を記憶するメモリを備え、

第１の処理データの全ブロックデータの復号処理が完了する前に第２の処理データの最初のブロックデータの復号処理を開始するとともに、第２の処理データの最初のブロックデータの復号処理を開始する場合に第１の処理データの復号処理の状態を上記メモリに記憶させ、第１の処理データの復号処理を再開する場合に復号装置の復号処理の状態をメモリに記憶した第１の処理データの復号処理の状態に復帰させてから第１の処理データの復号処理を再開することを特徴とする。

【００２７】

上記復号装置は、第２の処理データの全ブロックデータの復号処理の完了する前に第１の処理データの復号処理を再開するとともに、上記メモリは、第１の処理データの復号処理を再開する場合に第２の処理データの復号処理状態を記憶し、第２の処理データの復号処理を再開する場合は、復号装置の復号処理の状態をメモリに記憶した第２の処理データの復号処理の状態に復帰させてから第２の処理データの復号処理を再開することを特徴とする。

【００２８】

上記第１の処理データは、第１の暗号文であり、上記第２の処理データは、第２の暗号文であることを特徴とする。

【００２９】

上記復号装置は、割り込みにより第２の処理データの最初のブロックデータの復号処理を開始することを特徴とする。

【００３０】

この発明に係る復号装置は、暗号文Ｃを構成する暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）と暗号文Ｎを構成する暗号文ブロックデータN_j（ｊ＝１，２，３，・・・）とを復号する復号装置において、

暗号文Ｃの復号処理中に暗号文Ｎの復号要求を任意の時点で受け付けるメカニズムと、

復号処理を行い中間ブロックデータT_i又は平文ブロックデータM_iを出力する復号モジュールと、

復号モジュールから出力された中間ブロックデータT_i又は平文ブロックデータM_iをフィードバックラインを介し復号モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Ｎの復号要求を受け付け、暗号文Ｎのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されない場合、フィードバックされるブロックデータを記憶するメモリと、

暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号さ

れる場合は、上記フィードバックループのフィードバックラインによりフィードバックされるブロックデータを選択してフィードバックループに供給し、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されず、暗号文Ｎのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶されたブロックデータを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする。

【００３１】

上記メモリは、

複数の暗号文に対応した複数のレジスタと、

復号処理をする暗号文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする。

【００３２】

この発明に係る復号方法は、復号モジュールを用いて第１の暗号文Ｃの暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）を復号する工程と、

上記暗号文ブロックデータC_iを復号している途中で又は暗号文ブロックデータC_iを復号した後に、第１の暗号文Ｃの暗号文ブロックデータC_{i+1}の復号に用いられる中間ブロックデータT_i又は平文ブロックデータM_iをメモリに記憶する工程と、

上記暗号文ブロックデータC_{i+1}の復号に用いられるブロックデータをメモリに記憶した後に、第２の暗号文Ｎの少なくとも１つの暗号文ブロックデータを復号する工程と、

上記第２の暗号文Ｎの少なくとも１つの暗号文ブロックデータを復号した後に、メモリに記憶された、暗号文ブロックデータC_{i+1}の復号に用いられるブロックデータを入力し、復号モジュールを用いて第１の暗号文Ｃの暗号文ブロックデータC_{i+1}を復号する工程と

を備えたことを特徴とする。

【００３３】

この発明に係る復号装置は、１つ以上の暗号文ブロックデータからなる暗号文

を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

暗号文ブロックデータを復号したときに生成した中間ブロックデータT_i 又は平文ブロックデータM_i をフィードバックする第１のフィードバックループを有し、暗号文ブロックデータを入力し、第１のフィードバックループによりブロックデータをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と

を備えたことを特徴とする。

【００３４】

上記復号部と認証子生成部とは、１つの復号モジュールと、１つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

復号処理と認証生成処理とを交互に実行するために、メモリから復号処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクタと

を備えたことを特徴とする。

【００３５】

この発明に係る復号方法は、１つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

暗号文ブロックデータを復号したときに生成した中間ブロックデータT_i 又は平文ブロックデータM_i をフィードバックする第１のフィードバック工程を有し、暗号文ブロックデータを入力し、第１のフィードバックループによりブロックデータをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復

号工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、復号工程に入力される暗号文のブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成工程と

を備えたことを特徴とする。

【００３６】

【発明の実施の形態】

実施の形態１．

図１は、この実施の形態におけるＣＢＣモードの暗号化装置を示す図である。

この実施の形態の暗号化装置は、セレクタ５４と排他的論理和回路５８と暗号鍵Ｋを用いた暗号化モジュール５１とメモリ５５とにより構成されている。セレクタ５４と排他的論理和回路５８と暗号鍵Ｋを用いた暗号化モジュール５１は、フィードバックライン６５とフィードバックライン６６とフィードバックライン６７によりフィードバックループを構成している。暗号鍵Ｋを用いた暗号化モジュール５１により暗号化された暗号文ブロックデータC_iは、フィードバックループにより再び排他的論理和回路５８に入力され、暗号鍵Ｋを用いた暗号化モジュール５１に供給される。

【００３７】

メモリ５５は、フィードバックライン６５と並列に設けられている。メモリ５５は、レジスタ５６とスイッチ５７により構成されている。スイッチ５７は、暗号鍵Ｋを用いた暗号化モジュール５１の出力をレジスタ５６に入力させるか無視するかを切り替えるものである。この切り替えは、例えば、割り込みＩＴにより行われる。割り込みＩＴが発生した場合には、スイッチ５７はＥに接続され、割り込みＩＴが解除された場合には、スイッチ５７はＦに接続される。レジスタ５６は、Ｅを経由してきた暗号文ブロックデータC_iを入力して記憶するものである。レジスタ５６に記憶された暗号文ブロックデータC_iは、セレクタ５４に出力される。セレクタ５４は、Ａ，Ｂ，Ｃの３つの入力を有しており、いずれか１

つの入力を選択するものである。これらの選択は、後述するように割り込みＩＴに依存する。

【００３８】

図２は、図１に示した暗号化装置の動作手順を示す図である。

図３は、図１に示した暗号化装置の動作フローチャートである。

この暗号化装置が電源を投入された場合のセレクタ５４の入力はＡに設定されており、スイッチ５７はＥに接続されているものとする。また、平文Ｎの暗号化要求があるときは、割り込みＩＴが発生し、平文Ｎの暗号化要求が解除されるまで、割り込みＩＴがオンになり続けるものとする。時刻Ｔ０において、平文ブロックデータM_1 の暗号化処理がスタートする。時刻Ｔ０において、平文ブロックデータM_1 の暗号化がスタートした場合には、セレクタ５４の入力Ａから一旦イニシャルバリューＩＶが入力された後、セレクタ５４はＢに切り替わる。そして、時刻Ｘにおいて、平文ブロックデータN_1 の暗号化を要求する割り込みＩＴが発生したとする。時刻Ｔ１までに、暗号文ブロックデータC_1 はメモリ５５に記憶された状態になる。そして、割り込みＩＴの発生により時刻Ｔ１において、セレクタ５４は入力をＡに設定する。また、時刻Ｔ１において、スイッチ５７はＦに接続される。時刻Ｔ１以降は、平文ブロックデータN_1 の暗号化が行われ、暗号文ブロックデータD_1 が出力される。時刻Ｙにおいて、平文ブロックデータN_1 の暗号化が終了し、割り込みＩＴが解除されたものとする。この割り込みＩＴの解除により時刻Ｔ２において、セレクタ５４の入力はＣに切り替えられ、スイッチ５７はＥに接続される。セレクタ５４がＣに切り替わったことにより、メモリ５５に記憶されていた暗号文ブロックデータC_1 が平文ブロックデータM_2 の暗号化のために入力され、鍵Ｋを用いた暗号化モジュール５１により平文ブロックデータM_2 が暗号化されて、暗号文ブロックデータC_2 が出力される。時刻Ｔ３以前においては、セレクタ５４の入力はＢに切り替えられ、平文ブロックデータM_3 を暗号化する場合には、フィードバックループのフィードバックライン６５からフィードバックされた暗号文ブロックデータC_2 が入力され、鍵Ｋを用いた暗号化モジュール５１により平文ブロックデータM_2 暗号化されて、平文ブロックデータM_3 が暗号化され、暗号文ブロックデータC_3 が出力される。

【００３９】

図３のフローチャートを用いて全体の動作を説明する。

Ｓ１において、平文Ｍの暗号化処理がスタートし続行される。最後のブロックデータまで処理を終えた場合には、処理を終了する。Ｓ２において、任意の時点で生じる割り込みＩＴの発生が監視される。割り込みＩＴの発生がない場合には、Ｓ１の処理が続行される。平文ブロックデータM_iの処理中に割り込みＩＴが発生した場合には、Ｓ３において、現在処理中の平文ブロックデータM_iの暗号文ブロックデータC_iをメモリ５５のレジスタ５６に記憶する。Ｓ４において、割り込みＩＴにより暗号化処理の要求があった平文Ｎの暗号化処理を行う。このＳ４の暗号化処理は、Ｓ５に示すように、割り込みＩＴの解除があるまで連続して行われる。割り込みＩＴの解除があった場合には、Ｓ６において、メモリ５５のレジスタ５６に記憶した暗号文ブロックデータC_iを用いてM_{i+1}の暗号化処理を行う。それ以降の処理は、Ｓ１に戻り、暗号化処理が続行される。

【００４０】

図４は、セレクタ５４のオペレーション処理を示す図である。

電源がオンになった場合には、Ｓ１１に示すように、入力をＡに設定する。Ｓ１２において、暗号化がスタートした場合には、Ｓ１３において、入力をＢに設定する。即ち、フィードバックループのフィードバックライン６５によりフィードバックされる暗号文ブロックデータC_iが用いられる。Ｓ１４において、現在処理しているブロックデータが最後であるということが判定された場合には、Ｓ１１に戻り電源オンと同じ状態に戻る。Ｓ１５において、割り込みＩＴの発生が確認された場合には、Ｓ１６において、入力をＡに設定し、暗号化がスタートした場合には、Ｓ１８において、入力をＢに設定する。割り込みＩＴの解除があるまでは、入力がＢに設定されたままで動作する。即ち、フィードバックループのフィードバックライン６５によりフィードバックされる暗号文ブロックデータC_iが用いられる。Ｓ１９において、割り込みＩＴの解除があったことが検知された場合には、Ｓ２０において、入力をＣに設定する。この入力をＣに設定することにより、メモリ５５に記憶された暗号文ブロックデータC_iが入力されることになる。このＣからの入力による暗号化がスタートした場合には、Ｓ１３に戻り

入力をＢに設定する。

このようにして、割り込みＩＴの発生に基づき、セレクタ５４を切り替えることができる。

なお、平文Ｍの暗号化処理も、割り込みＩＴにより任意の時刻にスタートさせてもよい。

【００４１】

図５は、スイッチ５７の割り込み処理のフローチャートである。

電源がオンになった場合、そして、その後の最初の平文の暗号化処理の場合は、スイッチ５７はＥに接続される。そして、Ｓ３１において、割り込みＩＴが発生した場合には、スイッチ５７をＥからＦに接続する。そして、Ｓ３３において、割り込みＩＴの解除が検出された場合には、スイッチ５７をＦからＥに接続する。このようにして、スイッチ５７は、割り込みＩＴの発生から解除までは暗号文ブロックデータC_iを無視する。従って、メモリ５５のレジスタ５６には、割り込みＩＴが発生したときに生成された暗号文ブロックデータC_iが記憶され続けることになる。

【００４２】

メモリ５５は、割り込みＩＴが発生したときの暗号化装置の状態を記憶するメモリである。メモリ５５が暗号化処理の状態を記憶しておくことにより、あるデータの暗号化の最中に他のデータの暗号化を行った場合でも、再びあるデータの暗号化の処理に復帰することができる。即ち、メモリ５５に記憶されたデータを用いることにより、暗号化が中断されたときと全く同じ状態に暗号化装置を復帰させることができ、中断した暗号化処理を続行させることが可能になる。

【００４３】

図６は、メモリ５５の他の例を示す図である。

メモリ５５は、割り込み制御部５２と入力スイッチ９６と出力スイッチ９７と複数のレジスタ（ＲＥＧ１，２，３）を有している。このように、複数のレジスタを有することにより、複数の割り込みを受け付けることが可能になる。

【００４４】

図７は、メモリ５５の割り込み処理の動作を示す図である。

割り込みＩＴが発生すると、Ｓ４１において、現在使用中のレジスタｋの番号ｋを記憶する。Ｓ４２において、入力スイッチ９６と出力スイッチ９７をレジスタｋ以外のレジスタｌに接続する。この状態で、平文Ｎの暗号化が継続される。更に、平文Ｎの暗号化の最中に他の割り込みが発生したかを監視する。Ｓ４３において、他の割り込みＩＴが発生したことが検出された場合には、再び自分自身であるＳ４０の処理を呼び出す。このように、割り込みＩＴが発生するたびに、自分自身をＳ４０の処理をリカーシブに呼び出すことにより、複数階層の割り込み処理を行うことができる。Ｓ４４においては、割り込みが解除されたかを検出し、割り込みが解除された場合には、入力スイッチ９６と出力スイッチ９７を記憶しておいた番号ｋを用いてレジスタｋに切り替える。図６に示す場合は、３つのレジスタがあるので、３階層の割り込み処理を行うことができる。

【００４５】

図８は、メモリ５５の他の例を示す図である。

メモリ５５は、スタック６４を有している。スタック６４は、先入れ後出し（ＦＩＬＯ）のレジスタである。スタック１を使用中に割り込みＩＴが発生した場合には、スタック１のデータをスタック２に移し、それ以後のデータをスタック１に積み上げ、割り込みＩＴが解除された場合には、積み上げたスタック１のデータを出力し、スタック２のデータをスタック１に戻す。図８に示す場合は、４階層の割り込み処理を行える場合を示している。

【００４６】

図６に示すように、複数階層の割り込み処理を行うことができる場合は、各割り込みに対して優先度を付けることができる。例えば、割り込みＩＴ１を優先度１とし、割り込みＩＴ２を優先度Ｉより優先度の低い優先度２とすることにより、優先度１の割り込みＩＴ１が発生した場合には、優先度２の処理を遅らせることができる。

【００４７】

図９は、優先度１の暗号化処理を優先度２の暗号化処理に優先させた場合を示している。優先度１の暗号化処理を先に終了させている。

図１０は、優先度がともに等しい場合の暗号化処理の場合を示している。

優先度が等しい場合には、２つの平文の各ブロックデータを交互に暗号化する。

図１１は、優先度１のデータと２つの優先度２のデータを暗号化する場合を示している。

図９～図１１に示すように、割り込みに優先度を付けることによりユーザが望ましいと思われる暗号化処理手順を実現することができる。緊急用のデータや短いデータの場合には、優先度を高くすることにより効率のよい処理を行うことができる。

【００４８】

図１２は、メモリ５５をフィードバックライン６６と並列においた場合を示している。

第１セレクタ６１と第２セレクタ６２とにより、図１のセレクタ５４と同じ選択動作をさせる。

図１３は、メモリ５５をフィードバックライン６７と並列においた場合を示している。

図１４は、図１３の暗号化装置の動作手順を示す図である。

割り込みＩＴが発生した時刻Ｘが排他的論理和回路５８で排他的論理和演算される前である場合には、メモリ５５は、排他的論理和回路５８により排他的論理和演算された中間ブロックデータT_iを記憶する。そして、平文ブロックデータN_1を暗号化する。次に、メモリ５５に記憶された中間ブロックデータT_iを第２セレクタ６２により選択させ、暗号鍵Ｋを用いた暗号化モジュール５１に入力し、暗号化して暗号文ブロックデータC_1を出力する。

【００４９】

図１及び図１２及び図１３に示すように、メモリ５５は、フィードバックライン６５とフィードバックライン６６とフィードバックライン６７のいずれのラインと並列の設けられていても構わない。メモリ５５は、暗号化装置が、あるデータの暗号化処理中に他のデータの暗号化を開始するとき、他のデータの暗号化を開始する直前の状態を覚えておくものであり、他のデータの暗号化処理が終了した時点で、メモリ５５に記憶されたデータを用いて暗号化装置が元の状態に復帰

できるのであれば、メモリ５５は、どの場所に設けられていても構わない。また、メモリ５５は、複数箇所に設けられていてもよい。

【００５０】

図１５は、ＯＦＢモードの暗号化装置の構成図である。

図３４に比べて、メモリ５５が追加されている点が特徴である。

図１６は、ＣＦＢモードの暗号化装置を示す図である。

図３６に比べて、メモリ５５が設けられている点が特徴である。

【００５１】

図１７は、ＣＢＣモードの復号装置を示す図である。

図３３に比べて、メモリ７５が設けられている点が特徴である。

メモリ７５は、レジスタ７６とスイッチ７７により構成されている。

図１８は、図１７の復号装置の動作手順を示す図である。

暗号文ブロックデータC_1を復号している最中に割り込みＩＴの発生があった場合には、暗号文ブロックデータC_1がメモリ７５のレジスタ７６に記憶される。その後、暗号文ブロックデータD_1の復号が行われ、平文ブロックデータN_1が復号される。そして、メモリ７５のレジスタ７６に記憶された暗号文ブロックデータC_1が読み出され、暗号文ブロックデータC_2の復号が行われ、平文ブロックデータM_2が復号される。セレクタ７４の動作は、図４に示したものと同じである。また、スイッチ７７の動作は、図５に示したものと同じである。

【００５２】

図１９は、ＯＦＢモードの復号装置を示す図である。

図２０は、ＣＦＢモードの復号装置を示す図である。

【００５３】

前述した説明においては、３つのモードの場合の暗号化装置と復号装置を説明したが、前述した３つのモードは一例であり、これらのモードの改良されたもの、或いは、これらのモードが変形されたものであっても構わない。特に、特徴となる点は、先のブロックデータが暗号化復号されたときに生成されたブロックデータC_i又はM_i又はT_iが次のブロックデータM_{i+1}又はC_{i+1}の暗号化復号処理にフィードバックデータとして用いられる暗号化復号方法において、暗号化

復号の状態を記憶するメモリ５５を設け、他のデータの暗号化復号化の処理後にブロックデータC_i 又はM_i 又はT_i を用いて再び元の状態に復帰可能にできる点である。従って、特に暗号化モード、復号モードは問わない。

なお、割り込みＩＴを用いず、ポーリング方式やトークン取得方式等の他のメカニズムを用いて暗号化要求を受け付け、２以上の暗号化復号処理のインタラクティブな並列処理を行うようにしてもよい。

また、暗号鍵Ｋを用いる暗号化復号処理の場合を示したが、暗号鍵Ｋを用いない暗号化復号処理の場合でもよい。

【００５４】

実施の形態２．

この実施の形態においては、暗号化装置が秘匿処理とデータの完全性保証処理を行う場合について説明する。

データの秘匿処理とは、データを暗号化し、データが盗聴されても、或いは、盗まれても意味が分からなくすることである。また、データの完全性保証とは、データが何者かにより置き換えられていることがないことを保証することをいう。データを伝送する場合には、データの秘匿処理を行った上にデータの完全性を保証して伝送したい場合がある。データの秘匿処理は、データを暗号化することにより行われる。データの完全性保証処理は、データの最後に認証子（ＭＡＣ：Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を付加し、その認証子を検証することにより改竄を発見することにより行われる。

【００５５】

図２１は、ＯＦＢモードの暗号化部１００により秘匿処理を行い、ＣＢＣモードの認証子生成部２００により認証子（ＭＡＣ）を生成する場合を示している。

図２２は、図２１に示す暗号化装置の動作手順を示す図である。

平文ブロックデータM_1 が、まず暗号文ブロックデータC_1 に暗号化される。次に、平文ブロックデータM_2 が入力され、暗号文ブロックデータC_2 に暗号化される。この平文ブロックデータM_2 の暗号化と同じ時刻に暗号文ブロックデータC_1 が入力され、認証子の演算が始まる。時刻Ｔ１とＴ２の間に平文ブロックデータM_2 の暗号化と暗号文ブロックデータC_1 に基づく認証子演算が行われる

。また、時刻Ｔ２とＴ３の間では、平文ブロックデータM_3の暗号化と暗号文ブロックデータC_2に基づく認証子の演算が行われる。時刻Ｔ３においては、暗号文ブロックデータC_3に基づく認証子の演算が行われ、認証子Ｐが出力される。

図２１で特徴となる点は、排他的論理和回路５８から出力される暗号文ブロックデータC_iがフィードライン６９により排他的論理和回路５９に入力されている点である。フィードライン６９によりＯＦＢモードとＣＢＣモードの暗号化処理を結合することにより、図２２に示すように、秘匿処理と完全性認証処理がパイプライン処理で実行される。図４１に示した場合は、時刻Ｔ６で処理時間がかかったが、図２２の場合は、時刻Ｔ４で処理が終了して高速処理が行われたことになる。

【００５６】

図２３は、図２１に示した暗号化装置の動作フローチャート図である。

Ｓ５１において、ブロックデータカウンタｉを１とする。Ｓ５２は、暗号化部１００の動作であり、暗号化部１００は、平文ブロックデータM_iを入力して平文ブロックデータM_iを暗号化し、暗号文ブロックデータC_iを生成して暗号文ブロックデータC_iを出力する。Ｓ５３は、認証子生成部２００の動作であり、暗号文ブロックデータC_iを入力し暗号文ブロックデータC_iを暗号化し、認証子を演算する。Ｓ５４は、ブロックデータカウンタｉが最後のブロックデータｎを示しているかどうかを判断し、最後のブロックデータでない場合には、Ｓ５５において、ブロックデータカウンタｉを増加させ、再びＳ５２の処理に戻る。即ち、暗号化部１００と認証子生成部２００の処理を繰り返す。Ｓ５４において、最後のブロックデータの処理が終了した場合には、Ｓ５３で演算された直前の認証子が最終的な認証子であるから、Ｓ５６において、その認証子を暗号文ブロックデータC_iの最後に付加する。図２３に示すように、暗号化部１００が暗号文ブロックデータC_iを生成するたびに、認証子生成部２００が暗号文ブロックデータC_iを入力して認証子を演算することによりパイプライン処理が可能になり、高速処理が行われる。

【００５７】

図２４は、図２１に示した暗号化部１００と認証子生成部２００をあわせたも

のである。即ち、暗号化部１００と認証子生成部２００の暗号化モジュール５１を兼用し、また、暗号化部１００と認証子生成部２００の排他的論理和回路５８と５９を兼用したものである。更には、暗号化部１００のフィードバックライン６５と認証子生成部２００のフィードバックライン６６を兼用したものである。

【００５８】

第１セレクタ６１は、秘匿処理の開始時にイニシャルバリューＩＶを選択するものである。第２セレクタ６２は、完全性保証処理の開始時にイニシャルバリューＩＶを選択するものである。第３セレクタ６３は、秘匿処理と完全性保証処理を交互に選択するものである。第３セレクタ６３は入力をＥにすることにより、秘匿処理を行わせることができる。また、第３セレクタ６３は入力をＦにすることにより、完全性保証処理を行わせることができる。

メモリ９３は、暗号鍵Ｋを用いた暗号化モジュール５１から出力された中間ブロックデータT_iを記録するものである。メモリ９３は、入力スイッチ９６と出力スイッチ９７と第１レジスタ９８と第２レジスタ９９により構成されている。入力スイッチ９６と出力スイッチ９７は、第３セレクタ６３の切り替えと同期しており、第３セレクタ６３が切り替わるたびに入力スイッチ９６及び出力スイッチ９７も切り替わる。

【００５９】

図２５は、図２４に示す暗号化装置の動作手順を示す図である。

時刻Ｔ０とＴ１の間で平文ブロックデータM_1の秘匿処理が行われる。秘匿処理の途中で生成された中間ブロックデータは、第１レジスタ９８に記憶される。時刻Ｔ１とＴ２の間では、暗号文ブロックデータC_1に基づく認証子の演算が行われる。完全性保証処理により生成された認証子演算途中結果は、第２レジスタ９９に記憶される。次に、時刻Ｔ２とＴ３の間では、第１レジスタ９８に記憶された中間ブロックデータと平文ブロックデータM_2に基づいて平文ブロックデータM_2の秘匿処理が行われる。次に、時刻Ｔ３とＴ４の間では、第２レジスタ９９に記憶された認証子中間演算結果と暗号文ブロックデータC_2が入力され、認証子の演算が行われる。この動作を繰り返すことにより、秘匿処理と完全性認証処理が完了し、暗号文と認証子Ｐが出力される。図２５に示す場合は、時刻Ｔ６

までで処理が終了し、時間の短縮は図られていないが、図２４に示すように、暗号鍵Ｋを用いた暗号化モジュール５１と排他的論理和回路５８とフィードバックライン６７，６８（フィードバックループ）が兼用されているので、回路規模を小さくすることができる。

【００６０】

図２６は、ＯＦＢモードの復号化部３００とＣＢＣモードの認証子生成部４００を有する復号装置を示す図である。

この認証子生成部４００は、認証子生成部２００と同一構成のものである。

暗号文ブロックデータC_iは、復号化部３００の排他的論理和回路７８に入力されると同時に、フィードライン６９により認証子生成部４００に入力される。このような構成により、復号化部３００と認証子生成部４００の処理が同時並列実行され、処理速度が向上する。

【００６１】

図２７は、図２６に示した復号装置の復号化部３００と認証子生成部４００を一体化したものである。

図２７は、暗号鍵Ｋを用いた復号モジュール７１とフィードバックライン８７，８８（フィードバックループ）が兼用されている場合を示している。

第１セレクタ８１は、復号処理の開始時にイニシャルバリューＩＶを選択するものである。第２セレクタ８２は、完全性保証処理の開始時にイニシャルバリューＩＶを選択するものである。第３セレクタ８３は、復号処理と完全性保証処理を交互に選択するものである。第３セレクタ８３は入力をＥにすることにより、復号処理を行わせることができる。また、第３セレクタ８３は入力をＦにすることにより、完全性保証処理を行わせることができる。

メモリ９３は、暗号鍵Ｋを用いた暗号化モジュール５１から出力された中間ブロックデータT_iを記録するものである。メモリ９３は、入力スイッチ９６と出力スイッチ９７と第１レジスタ９８と第２レジスタ９９により構成されている。入力スイッチ９６と出力スイッチ９７は、第３セレクタ８３の切り替えと同期しており、第３セレクタ８３が切り替わるたびに入力スイッチ９６及び出力スイッチ９７も切り替わる。

【００６２】

図２８は、図２７に示した復号装置の動作手順を示す図である。

時刻Ｔ０とＴ１の間で暗号文ブロックデータC_1の復号処理と暗号文ブロックデータC_1のレジスタ１１１への保存が行われる。復号処理の途中で生成された中間ブロックデータは、第１レジスタ９８に記憶される。時刻Ｔ１とＴ２の間では、レジスタ１１１に保存された暗号文ブロックデータC_1に基づく認証子の演算が行われる。完全性保証処理により生成された認証子演算途中結果は、第２レジスタ９９に記憶される。次に、時刻Ｔ２とＴ３の間では、暗号文ブロックデータC_2がレジスタ１１１に保存され、第１レジスタ９８に記憶された中間ブロックデータと暗号文ブロックデータC_2に基づいて平文ブロックデータM_2の復号処理が行われる。次に、時刻Ｔ３とＴ４の間では、第２レジスタ９９に記憶された認証子中間演算結果とレジスタ１１１に保存された暗号文ブロックデータC_2が入力され、認証子の演算が行われる。この動作を繰り返すことにより、復号処理と完全性認証処理が完了し、平文と認証子Ｐが出力される。

【００６３】

図２９は、前述した暗号化装置又は復号装置の実装形式を示す図である。

図２９は、ＦＰＧＡ又はＩＣ又はＬＳＩの中に前述した暗号化装置及び復号装置が実現されている場合を示している。即ち、前述した暗号化装置及び復号装置は、ハードウェアで実現することができる。また、図示していないが、プリントサーキットボードにより実現することも可能である。

【００６４】

図３０は、前述した暗号化装置及び復号装置をソフトウェアで実現する場合を示している。

前述した暗号化装置は、暗号化プログラム４７で実現することができる。暗号化プログラム４７は、ＲＯＭ４２に記憶されている。暗号化プログラム４７は、サブルーチンとして機能する。暗号化プログラム４７は、ＲＡＭ４５に記憶されたアプリケーションプログラム４６からサブルーチンコールにより呼び出されて実行される。或いは、暗号化プログラム４７は、割り込み制御部４３で受け付ける割り込みの発生により起動されるようにしても構わない。メモリ５５は、ＲＡ

Ｍ４５の一部であっても構わない。アプリケーションプログラム４６、暗号化プログラム４７は、ＣＰＵ４１により実行されるプログラムである。

【００６５】

図３１は、アプリケーションプログラム４６が暗号化プログラム４７を呼び出すメカニズムを示している。

アプリケーションプログラム４６は、鍵Ｋとイニシャルバリュー ＩＶと平文Ｍと暗号文Ｃをパラメータにして暗号化プログラム４７を呼び出す。暗号化プログラム４７は、鍵Ｋとイニシャルバリュー ＩＶと平文Ｍを入力し、暗号文Ｃを返すものである。暗号化プログラム４７と復号プログラムが同一のときは、鍵Ｋとイニシャルバリュー ＩＶと暗号文Ｃと平文Ｍをパラメータにして暗号化プログラム４７を呼び出す。

また、図示しないが、暗号化プログラム４７は、デジタルシグナルプロセッサと、そのデジタルシグナルプロセッサにより読み込まれて実行されるプログラムによって実現しても構わない。即ち、ハードウェアとソフトウェアの組み合わせによって暗号化プログラム４７を実現しても構わない。

【００６６】

図２９，図３０，図３１は、主として、暗号化装置の場合を説明したが、復号装置でも同様の方式で実現できる。

【００６７】

図２９及び図３０に示したような暗号化装置及び復号装置は、電子機器に対してインストールすることができる。例えば、パーソナルコンピュータやファクシミリ装置や携帯電話やビデオカメラやデジタルカメラやテレビカメラ等のあらゆる電子機器にインストールすることができる。特に、この実施の形態における特徴が発揮できるのは、複数のチャネルからのデータを暗号化復号する場合に有効である。或いは、複数のユーザからのデータがアットランダムに到着して復号する場合に、或いは、複数のユーザに対するデータがアットランダムに発生して、それぞれのデータをリアルタイムに暗号化するような場合に有効である。即ち、暗号化復号するデータの数に比べて暗号化復号する装置の数が少ない場合に、前述した実施の形態の暗号化装置、復号装置が非常に有効である。例えば、多くの

クライアントコンピュータをサポートしなければならないサーバコンピュータや多くの携帯電話機からのデータを集配しなければならない基地局や回線コントローラなどに、前述した暗号化装置や復号装置が非常に有効である。

【００６８】

なお、暗号化処理同士及び復号処理同士の並列処理でなく、暗号化処理と復号処理との並列処理を行うようにしてもよい。

【００６９】

また、ＯＦＢモードの暗号化部（又は復号化部）とＣＢＣモードの認証子生成部との組み合わせの場合を示したが、ＯＦＢモードとＣＢＣモードとＣＦＢモードとこれらのモードの改良モードとその他のモードとのいずれのモードの組み合わせでも構わない。

【００７０】

また、認証子生成部が、暗号鍵Ｋを用いた暗号化を行う場合を示したが、認証子生成部は、データの攪拌や演算やその他のデータ処理を行う場合であっても構わない。

【００７１】

【発明の効果】

以上のように、この発明の好適な実施の形態によれば、平文Ｍの暗号化の途中で平文Ｎの暗号化を開始することができる。また、暗号文Ｃの復号中に他の暗号文Ｄの復号を開始することができる。

【００７２】

また、この発明の好適な実施の形態によれば、優先度を付けることにより暗号化復号されるデータを優先度に基づいて高速に処理することができる。

【００７３】

また、この発明の好適な実施の形態によれば、秘匿処理と完全性保証処理とを並列処理することにより高速処理が行える。また、秘匿処理と完全性保証処理を統合化された１つのハードウェアで行うことができる。

【図面の簡単な説明】

【図１】　実施の形態１のＣＢＣモードの暗号化装置を示す図。

【図２】　ＣＢＣモードの暗号化装置の動作手順を示す図。

【図３】　ＣＢＣモードの暗号化装置の動作フローチャート図。

【図４】　セレクタ５４の動作フローチャート図。

【図５】　スイッチ５７の割り込み処理フローチャート図。

【図６】　メモリ５５の他の例を示す図。

【図７】　メモリ５５の割り込み処理フローチャート図。

【図８】　メモリ５５の他の例を示す図。

【図９】　優先度処理を示す図。

【図１０】　優先度処理を示す図。

【図１１】　優先度処理を示す図。

【図１２】　メモリ５５がフィードバックライン６６と並列に設けられている図。

【図１３】　メモリ５５がフィードバックライン６７に並列に設けられている図。

【図１４】　図１３の暗号化装置の動作手順を示す図。

【図１５】　ＯＦＢモードの暗号化装置を示す図。

【図１６】　ＣＦＢモードの暗号化装置を示す図。

【図１７】　ＣＢＣモードの復号装置を示す図。

【図１８】　ＣＢＣモードの復号装置の動作手順を示す図。

【図１９】　ＯＦＢモードの復号装置を示す図。

【図２０】　ＣＦＢモードの復号装置を示す図。

【図２１】　実施の形態２の暗号化部１００と認証子生成部２００を有する暗号化装置を示す図。

【図２２】　暗号化部１００と認証子生成部２００を有する暗号化装置の動作手順を示す図。

【図２３】　暗号化部１００と認証子生成部２００を有する暗号化装置のフローチャート図。

【図２４】　暗号化部１００と認証子生成部２００を１つにした暗号化装置を示す図。

【図２５】　暗号化部１００と認証子生成部２００を１つにした暗号化装置の動作手順を示す図。

【図２６】　復号化部３００と認証子生成部４００を有する復号装置を示す図。

【図２７】　復号化部３００と認証子生成部４００を１つにした復号装置を示す図。

【図２８】　復号化部３００と認証子生成部４００を１つにした復号装置の動作手順を示す図。

【図２９】　暗号化装置及び復号装置のハードウェア実現例を示す図。

【図３０】　暗号化装置及び復号装置のハードウェア実現例を示す図。

【図３１】　アプリケーションプログラム４６により暗号化プログラム４７が呼び出される場合を示す図。

【図３２】　従来のＣＢＣモードの暗号化装置を示す図。

【図３３】　従来のＣＢＣモードによる復号装置を示す図。

【図３４】　従来のＯＦＢモードの暗号化装置を示す図。

【図３５】　従来のＯＦＢモードによる復号装置を示す図。

【図３６】　従来のＣＦＢモードの暗号化装置を示す図。

【図３７】　従来のＣＦＢモードによる復号装置を示す図。

【図３８】　従来の暗号化手順を示す図。

【図３９】　従来の暗号化手順を示す図。

【図４０】　秘匿処理と完全性保証処理を説明する図。

【図４１】　従来の秘匿処理と完全性保証処理の動作手順を示す図。

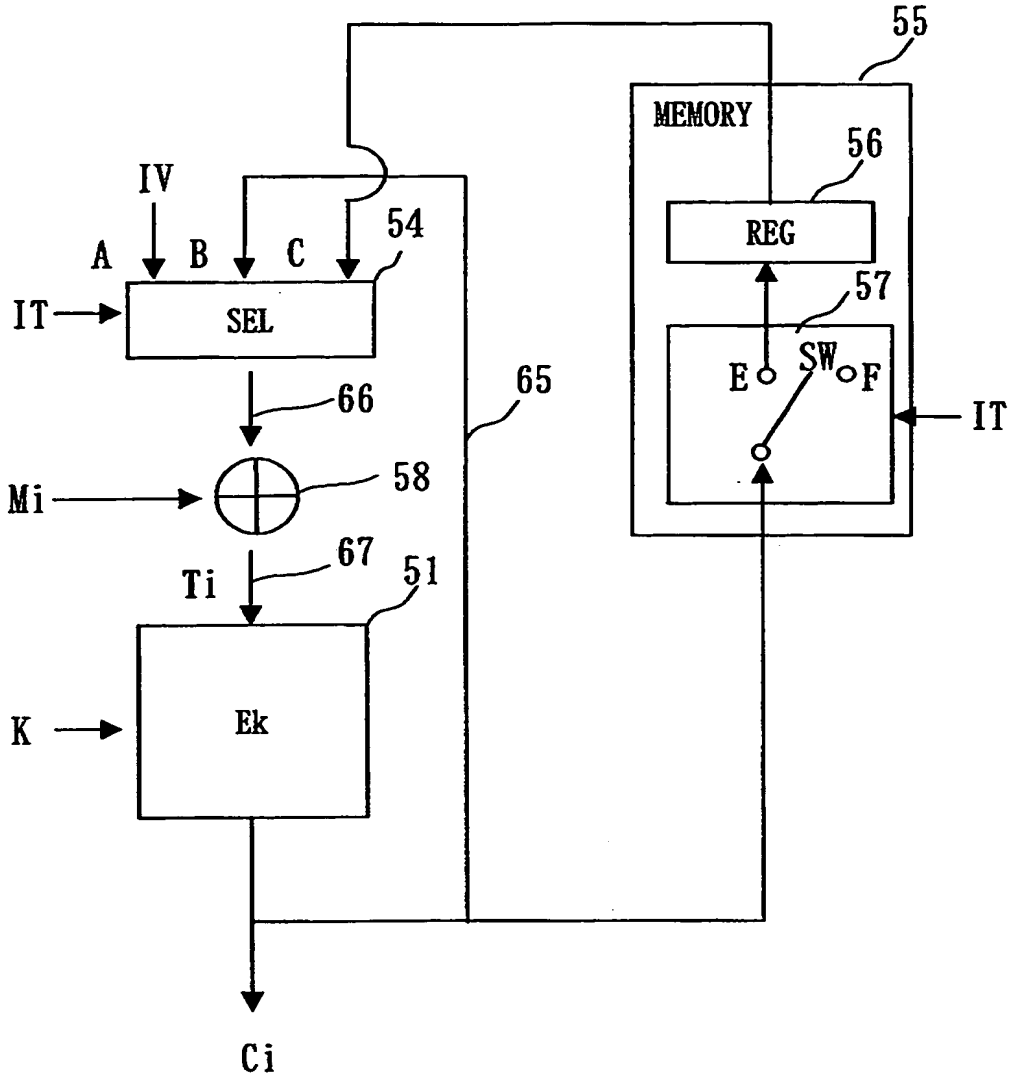
【符号の説明】

４１　ＣＰＵ、４２　ＲＯＭ、４３，５２　割り込み制御部、４５　ＲＡＭ、４６　アプリケーションプログラム、４７　暗号化プログラム、５１　暗号鍵Ｋを用いた暗号化モジュール、５３，５４，７３，７４　セレクタ、５５，７５，９５　メモリ、５６，７６　レジスタ、５７，７７　スイッチ、５８，５９，７８，７９　排他的論理和回路、６１，８１　第１セレクタ、６２，８２　第２セレクタ、６３，８３　第３セレクタ、６４　スタック、６５，６６，６７，６８

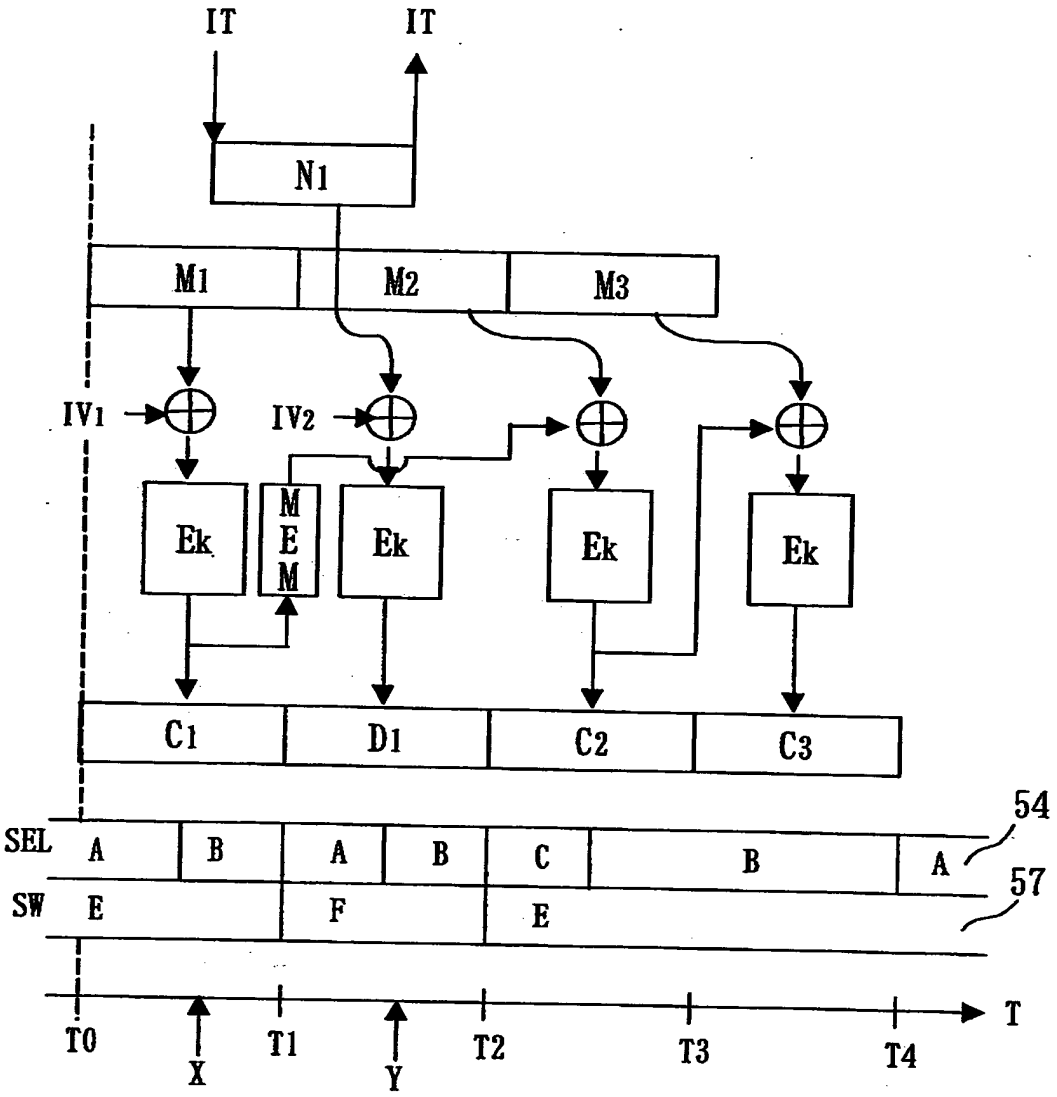
，８５，８６，８７，８８　フィードバックライン、６９，８９　フィードライン、７１　暗号鍵Ｋを用いた復号モジュール、９３　第１スイッチ、９４　第２スイッチ、９６　入力スイッチ、９７　出力スイッチ、９８　第１レジスタ、９９　第２レジスタ、１１１　レジスタ、C_1，C_2，C_3，C_i，D_1　暗号文ブロックデータ、F_i　フィードバックブロックデータ、ＩＴ　割り込み、ＩＶ　イニシャルバリュー、N_1，M_1，M_2，M_3，M_i　平文ブロックデータ、Ｐ　認証子、Ｔ，Ｘ，Ｙ　時刻、T_i　中間ブロックデータ。

【書類名】　　図面

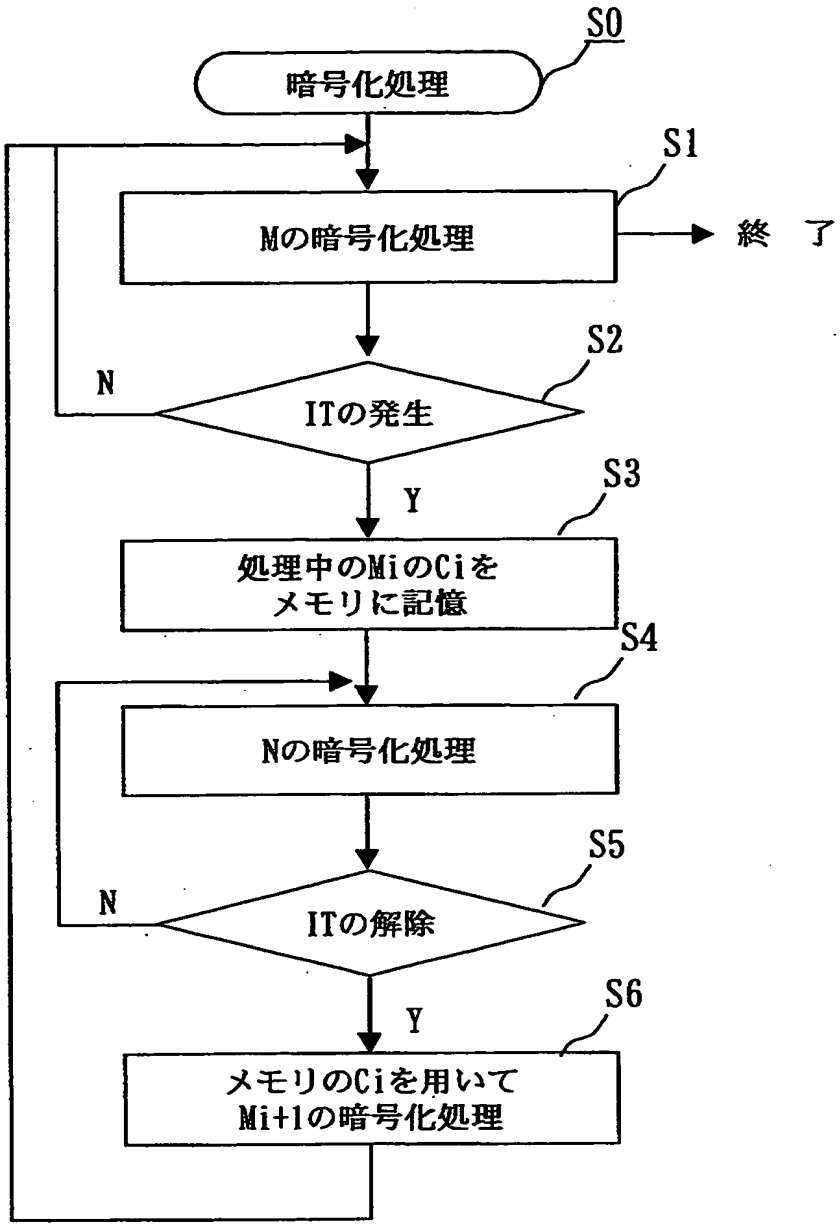
【図１】


55
MEMORY
56
REG
57
E
SW
F
IT
IV
A
B
C
54
IT
SEL
65
66
Mi
58
67
Ti
51
K
Ek
Ci

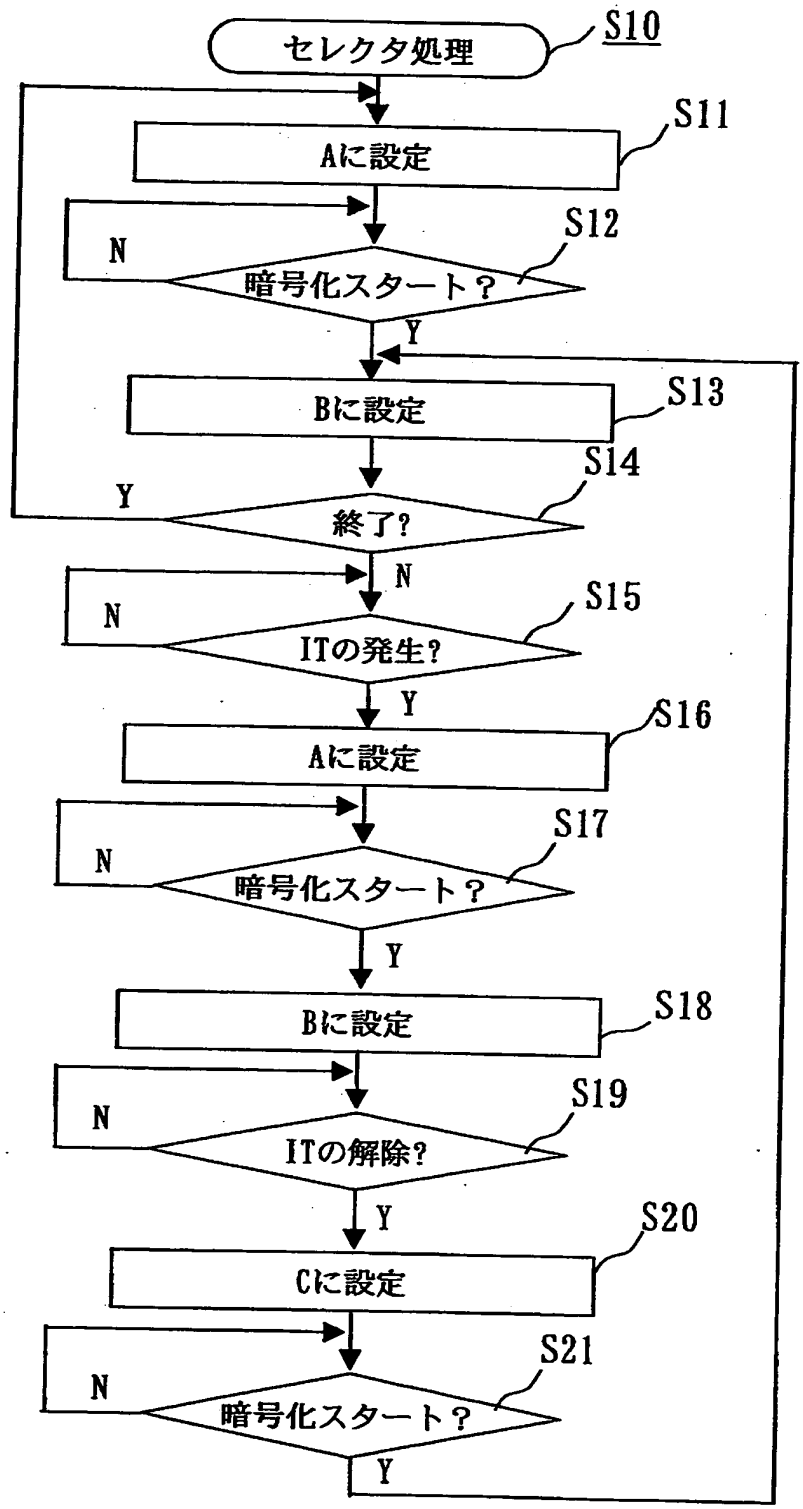
【図２】


IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
C1
D1
C2
C3
54
SEL
A
B
A
B
C
B
A
57
SW
E
F
E
T
T0
X
T1
Y
T2
T3
T4

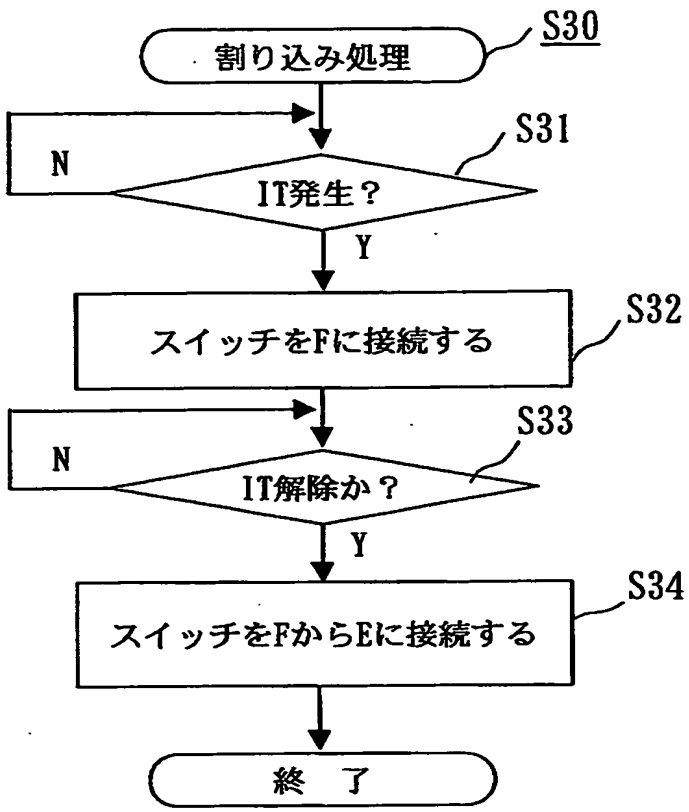
【図３】


S0
暗号化処理
S1
Mの暗号化処理
終　了
S2
N
ITの発生
Y
S3
処理中のMiのCiを
メモリに記憶
S4
Nの暗号化処理
S5
N
ITの解除
Y
S6
メモリのCiを用いて
Mi+1の暗号化処理

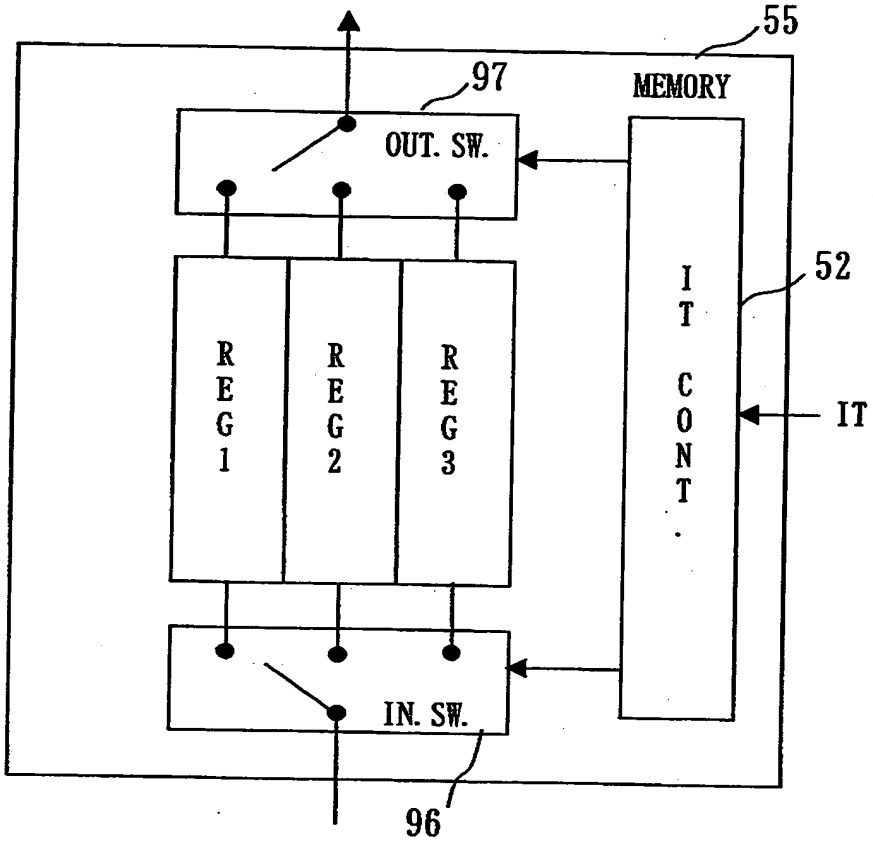
【図４】


セレクタ処理
S10
Aに設定
S11
N
暗号化スタート？
S12
Y
Bに設定
S13
Y
終了?
S14
N
N
ITの発生?
S15
Y
Aに設定
S16
N
暗号化スタート？
S17
Y
Bに設定
S18
N
ITの解除?
S19
Y
Cに設定
S20
N
暗号化スタート？
S21
Y

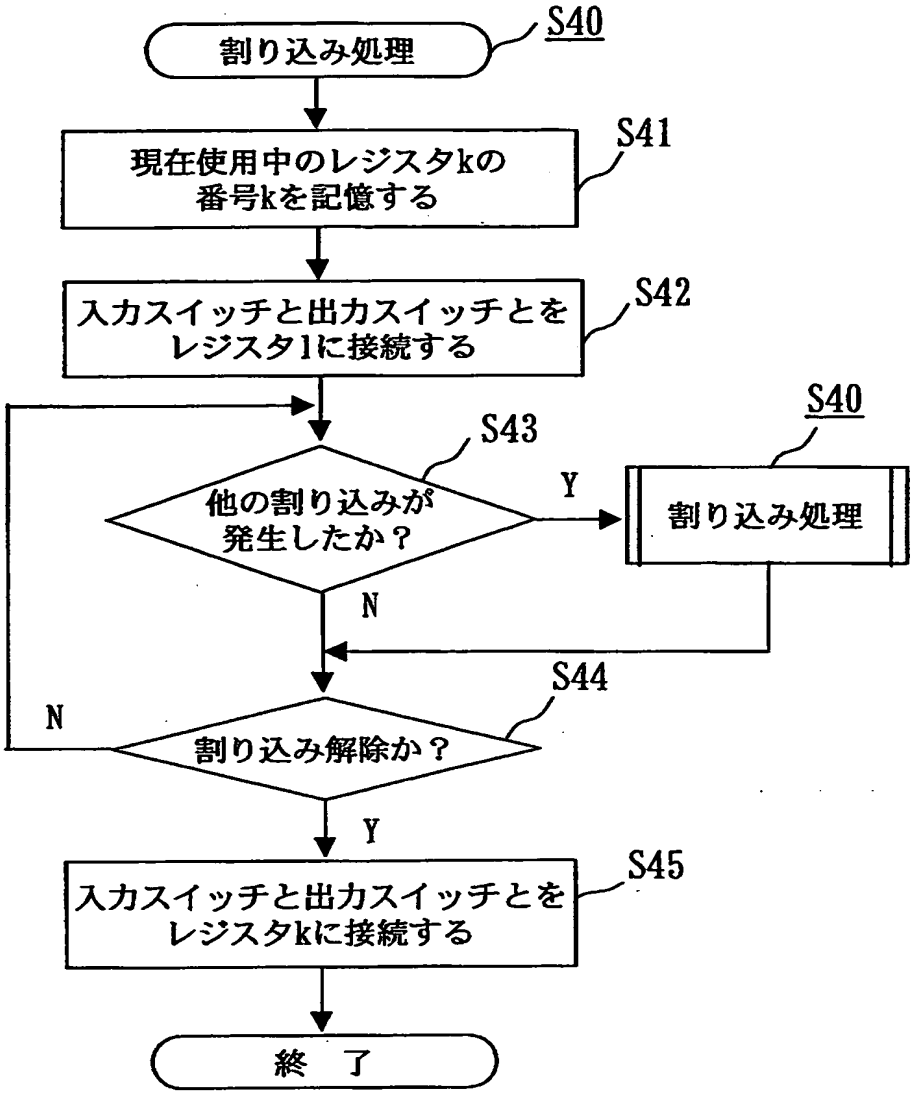
【図５】


割り込み処理
S30
S31
N
IT発生？
Y
スイッチをFに接続する
S32
S33
N
IT解除か？
Y
スイッチをFからEに接続する
S34
終　了

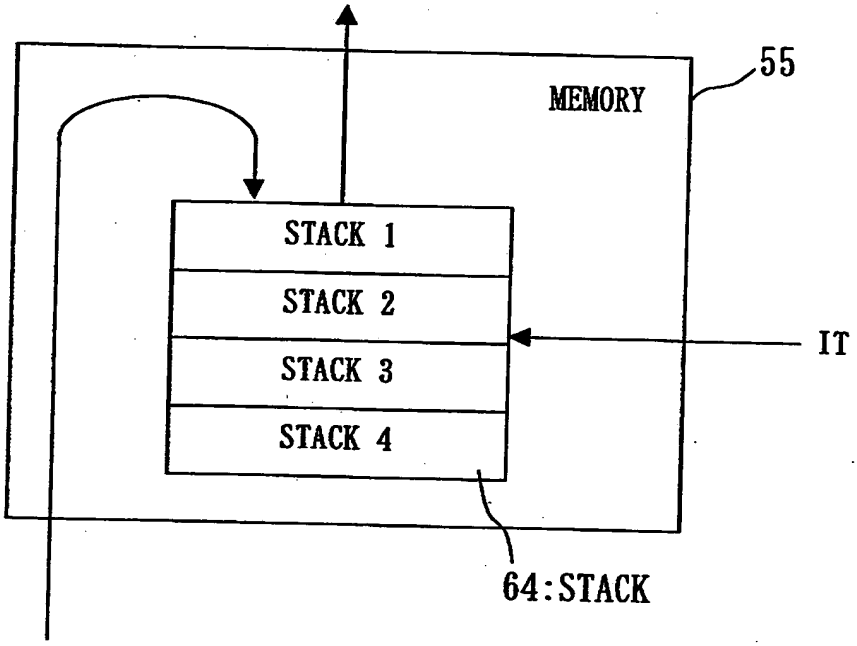
【図６】



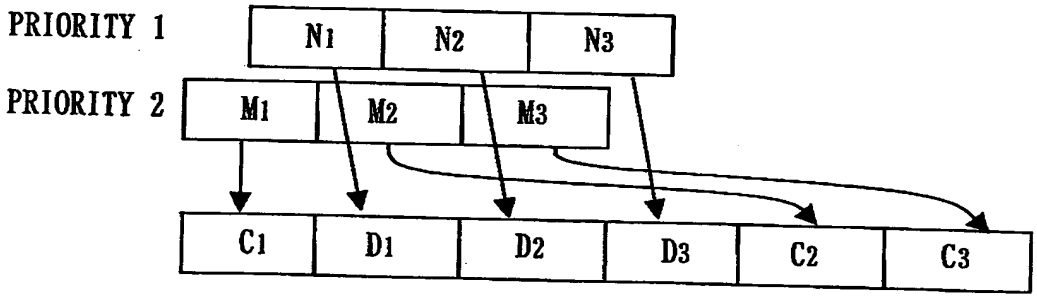
【図７】


割り込み処理
S40
現在使用中のレジスタkの
番号kを記憶する
S41
入力スイッチと出力スイッチとを
レジスタ1に接続する
S42
S43
他の割り込みが
発生したか？
Y
S40
割り込み処理
N
S44
N
割り込み解除か？
Y
S45
入力スイッチと出力スイッチとを
レジスタkに接続する
終　了

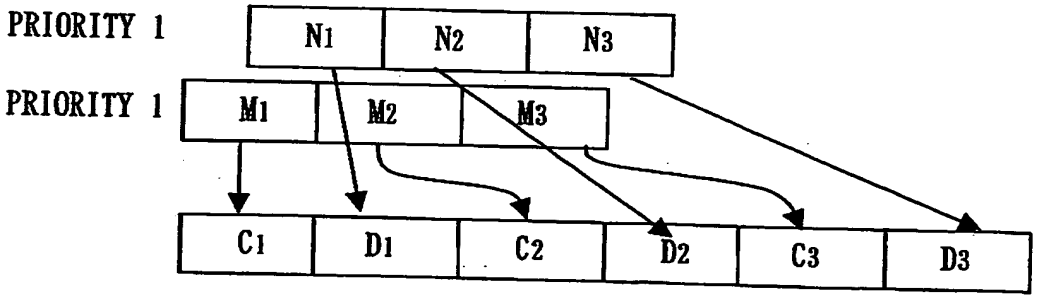
【図８】


MEMORY
55
STACK 1
STACK 2
STACK 3
STACK 4
IT
64:STACK

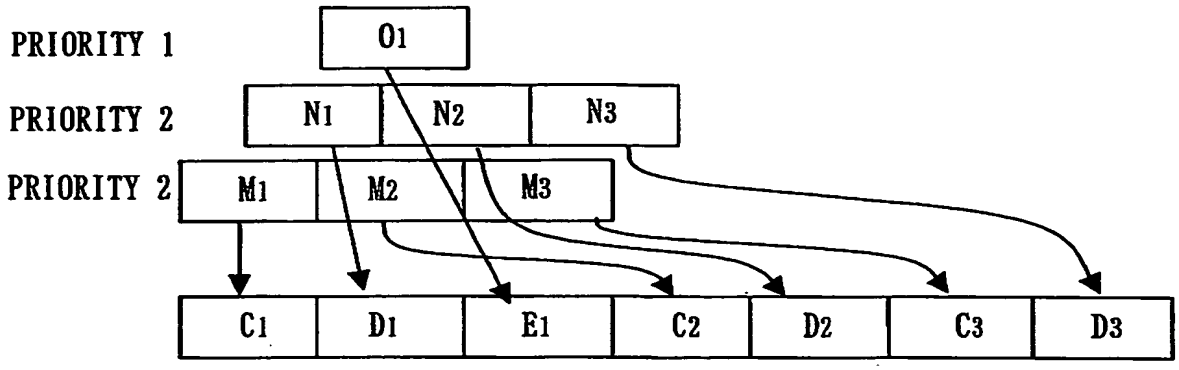
【図９】


PRIORITY 1
PRIORITY 2
N1
N2
N3
M1
M2
M3
C1
D1
D2
D3
C2
C3

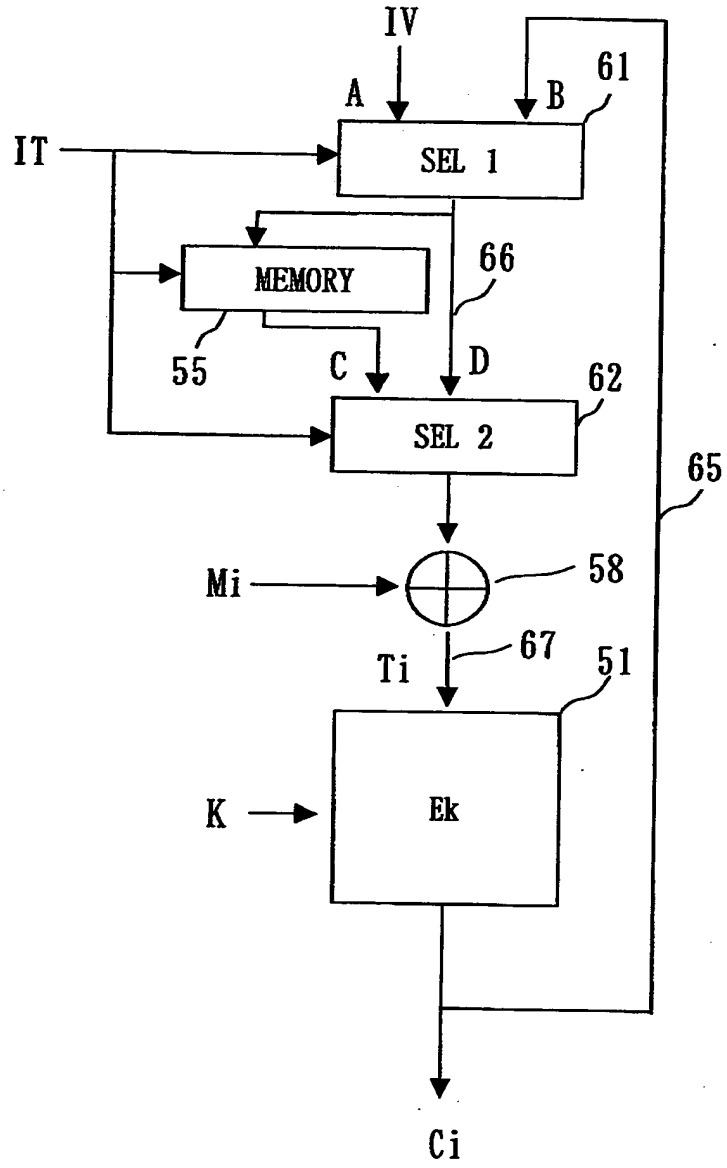
【図１０】


PRIORITY 1
PRIORITY 1
N1
N2
N3
M1
M2
M3
C1
D1
C2
D2
C3
D3

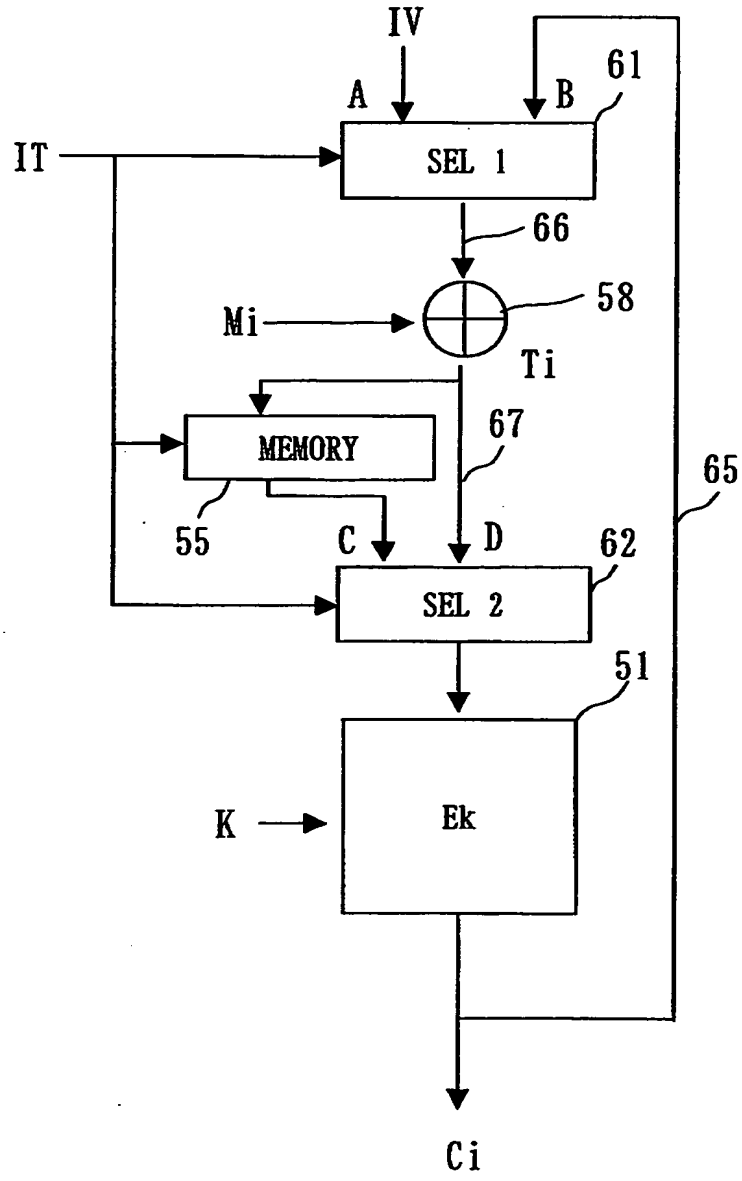
【図１１】


PRIORITY 1
PRIORITY 2
PRIORITY 2
O1
N1
N2
N3
M1
M2
M3
C1
D1
E1
C2
D2
C3
D3

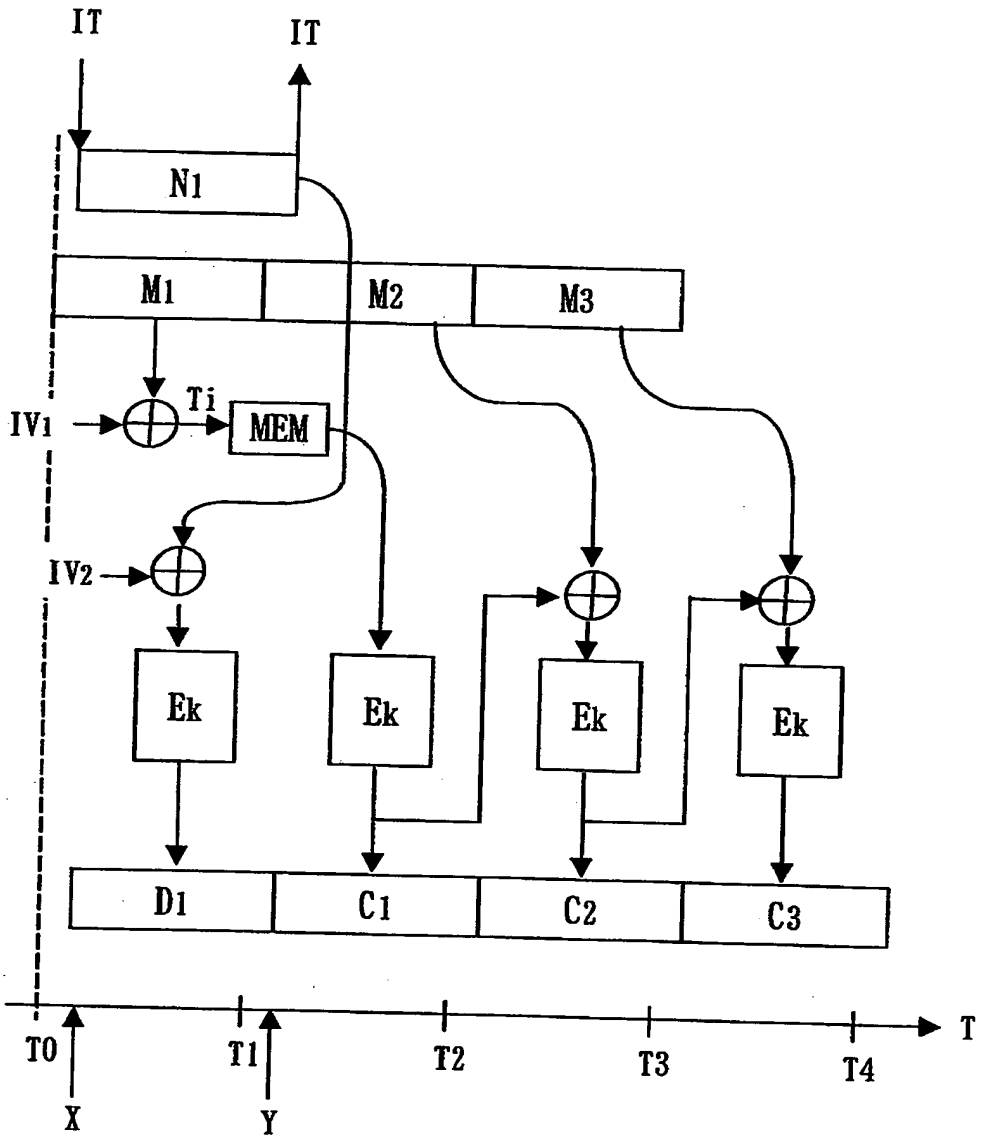
【図１２】



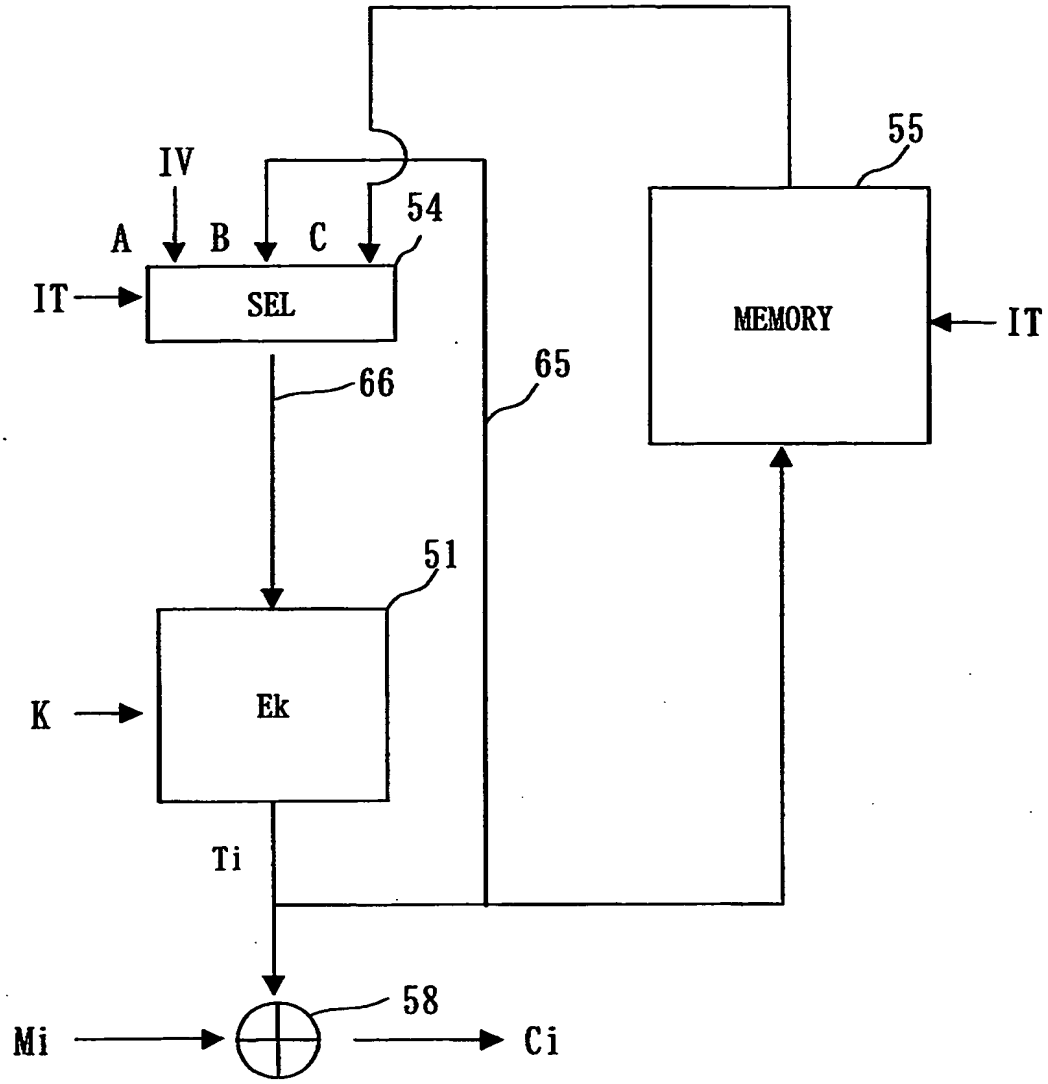
【図１３】



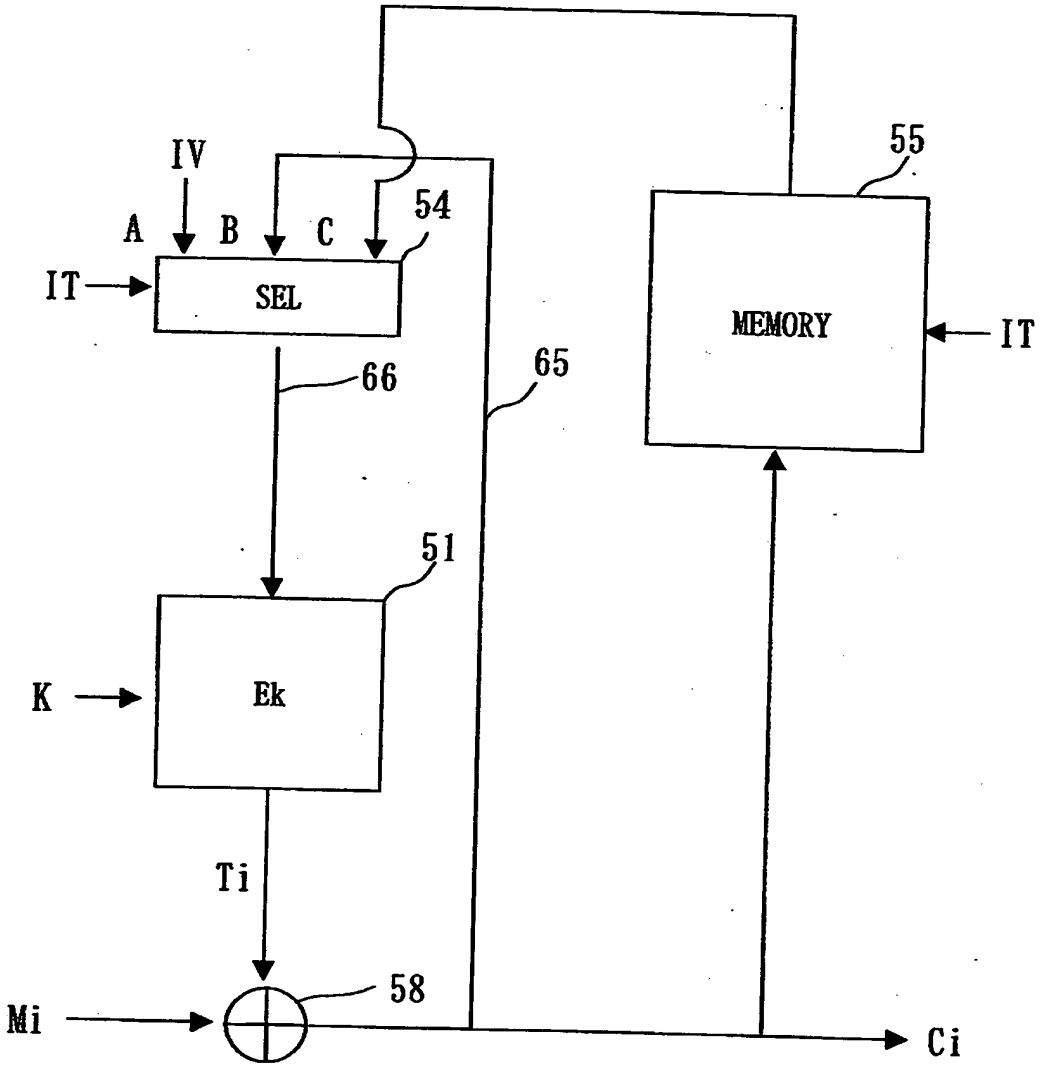
【図１４】


IT
IT
N1
M1
M2
M3
IV1
Ti
MEM
IV2
Ek
Ek
Ek
Ek
D1
C1
C2
C3
T
T0
T1
T2
T3
T4
X
Y

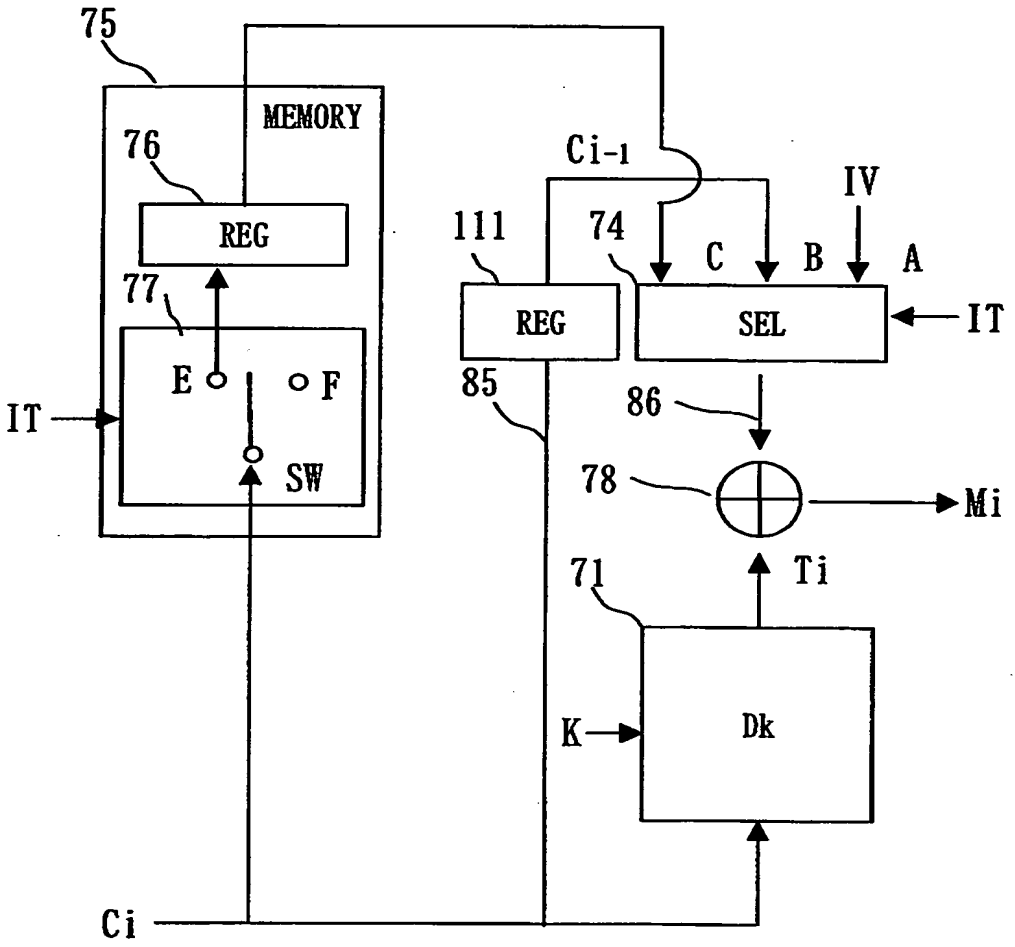
【図１５】



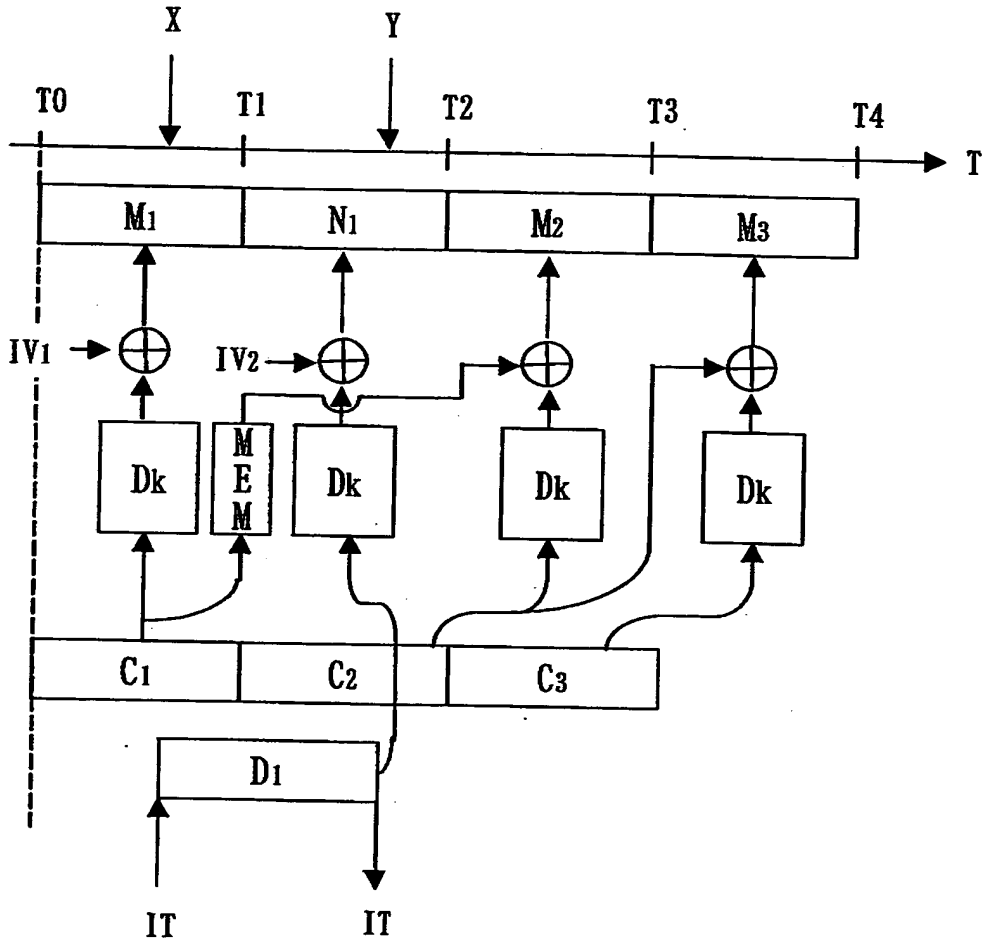
【図１６】



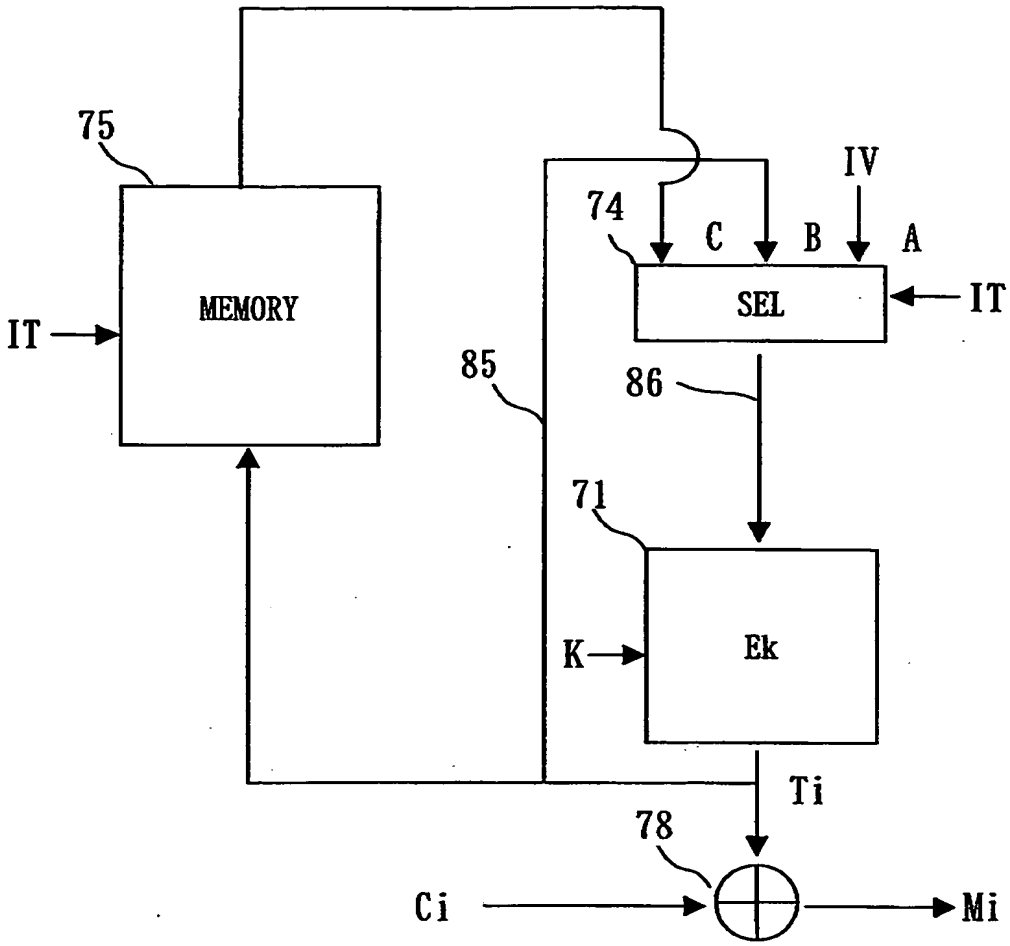
【図１７】


75
MEMORY
76
REG
77
E
F
SW
IT
Ci
Ci-1
111
74
C
B
A
IV
REG
SEL
IT
85
86
78
Mi
71
Ti
K
Dk

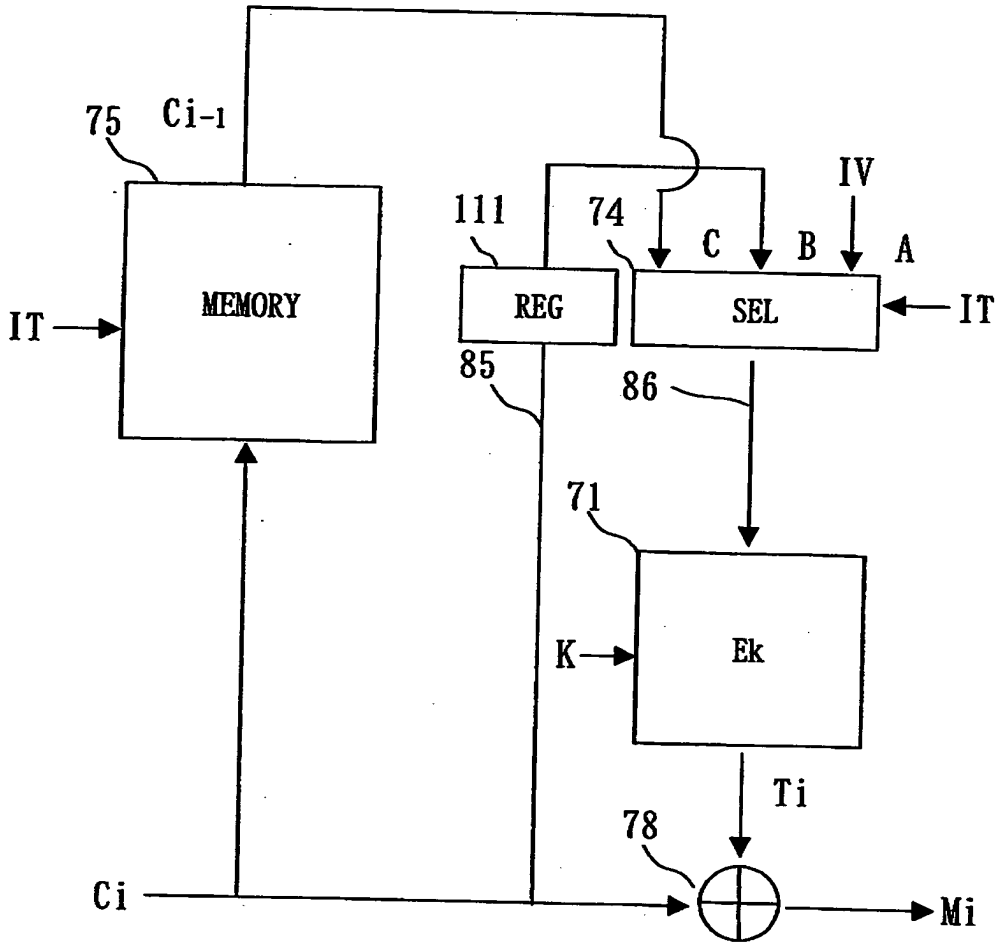
【図１８】


X
Y
T0
T1
T2
T3
T4
T
M1
N1
M2
M3
IV1
IV2
Dk
MEM
Dk
Dk
Dk
C1
C2
C3
D1
IT
IT

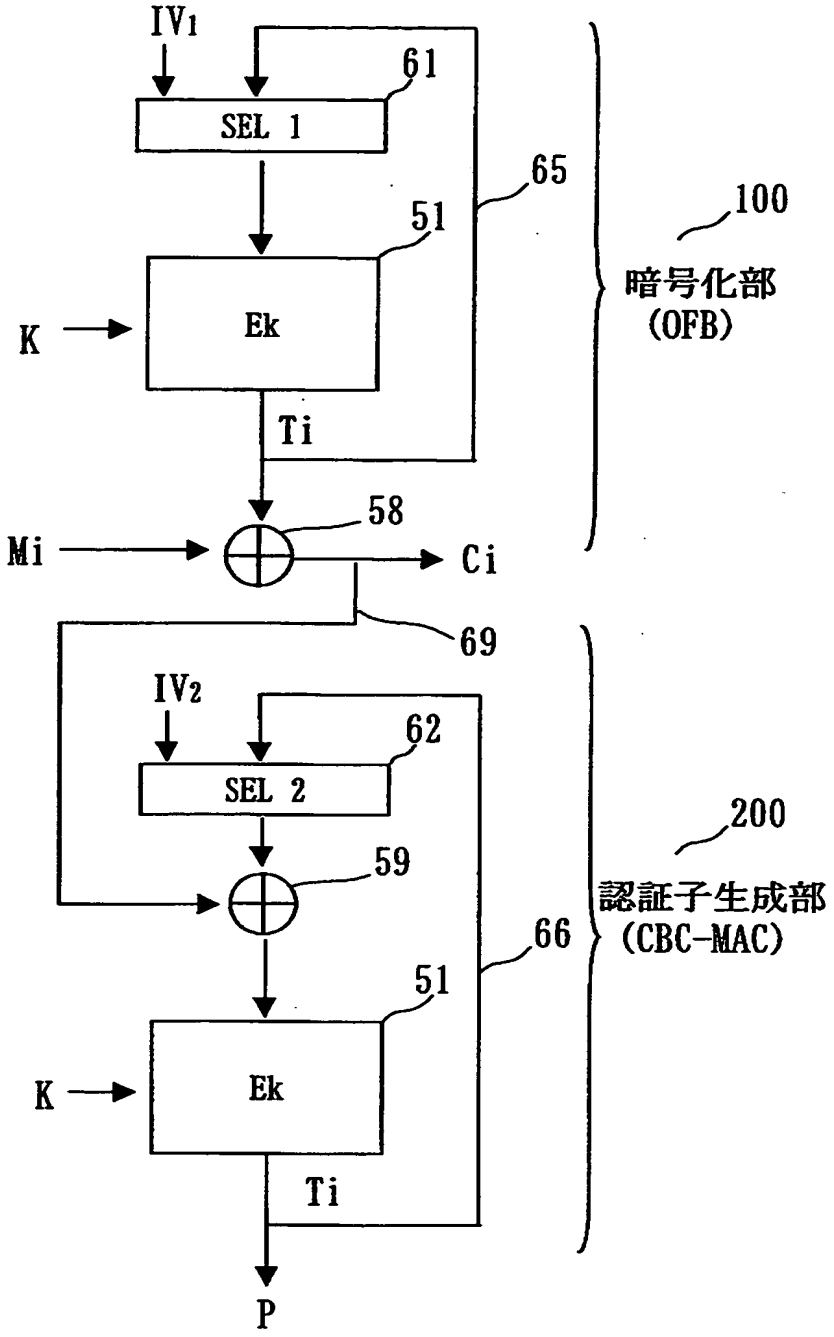
【図１９】



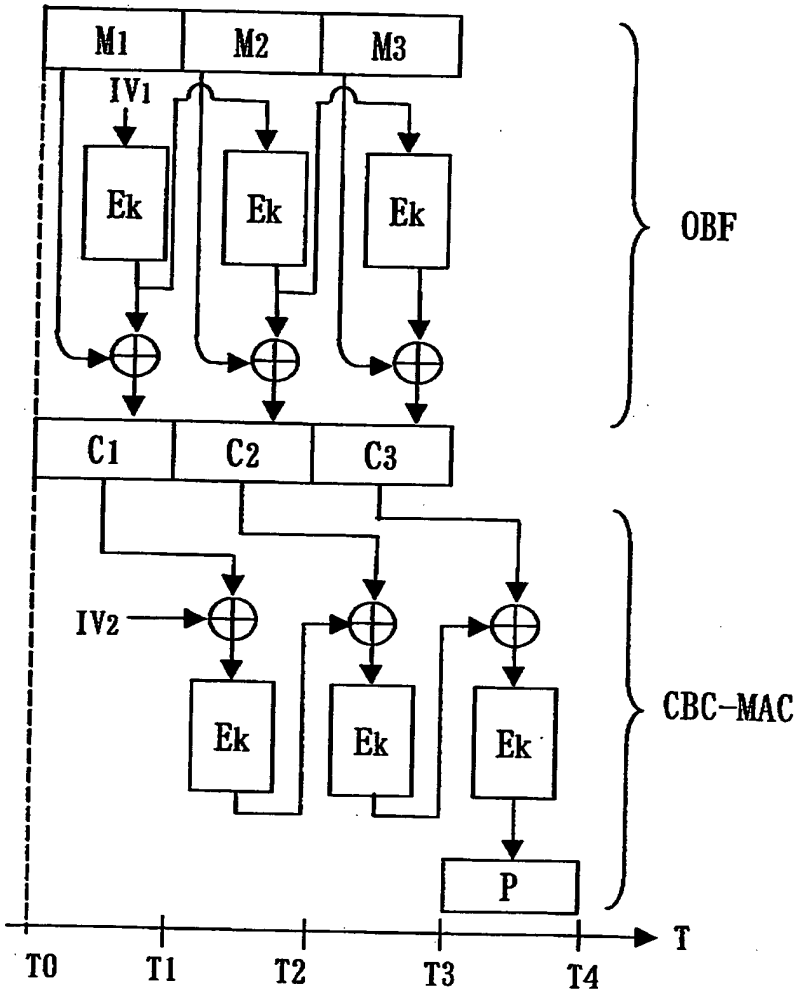
【図２０】



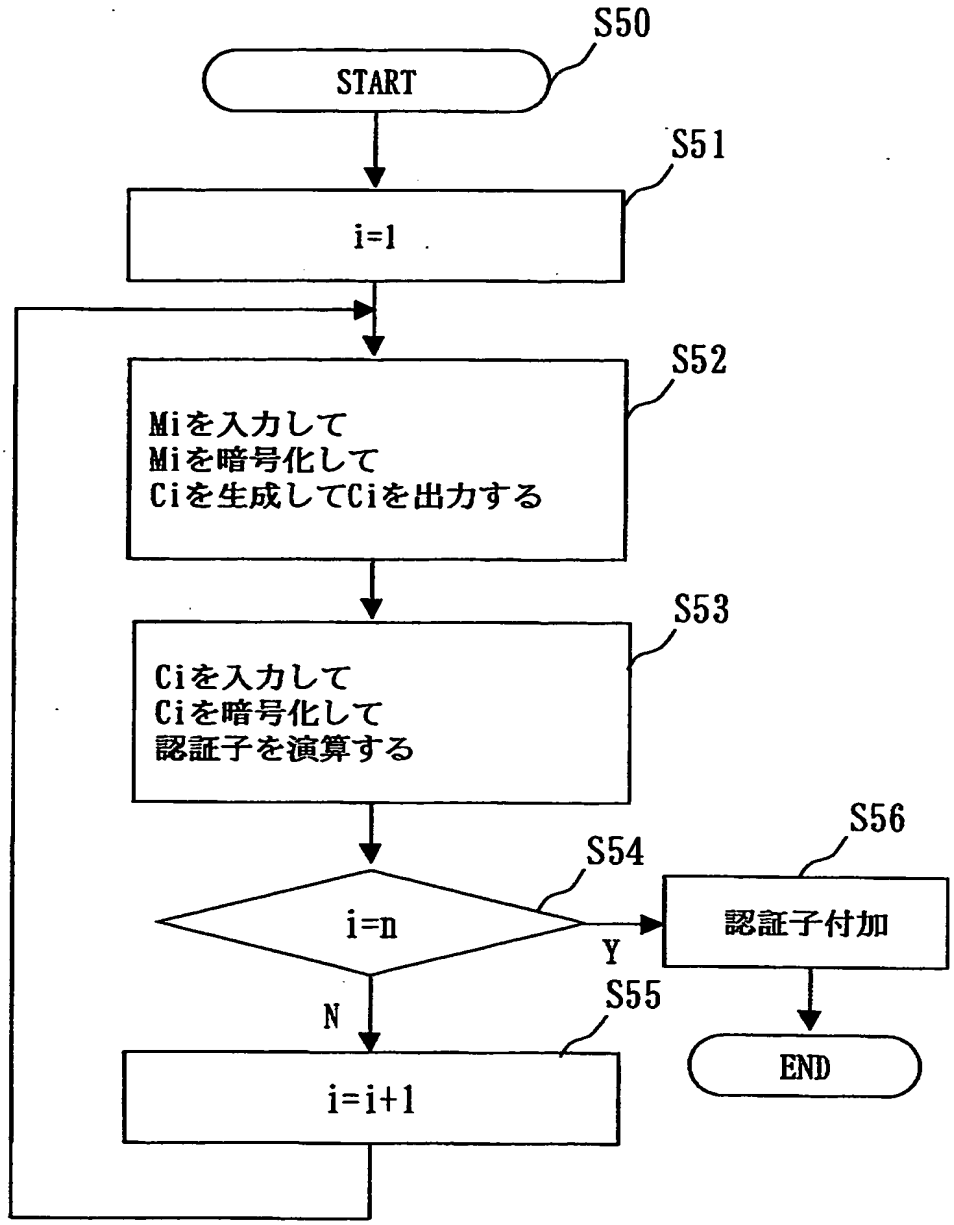
【図２１】


IV1
61
SEL 1
65
100
51
暗号化部
(OFB)
K
Ek
Ti
58
Mi
Ci
69
IV2
62
SEL 2
200
59
認証子生成部
(CBC-MAC)
66
51
K
Ek
Ti
P

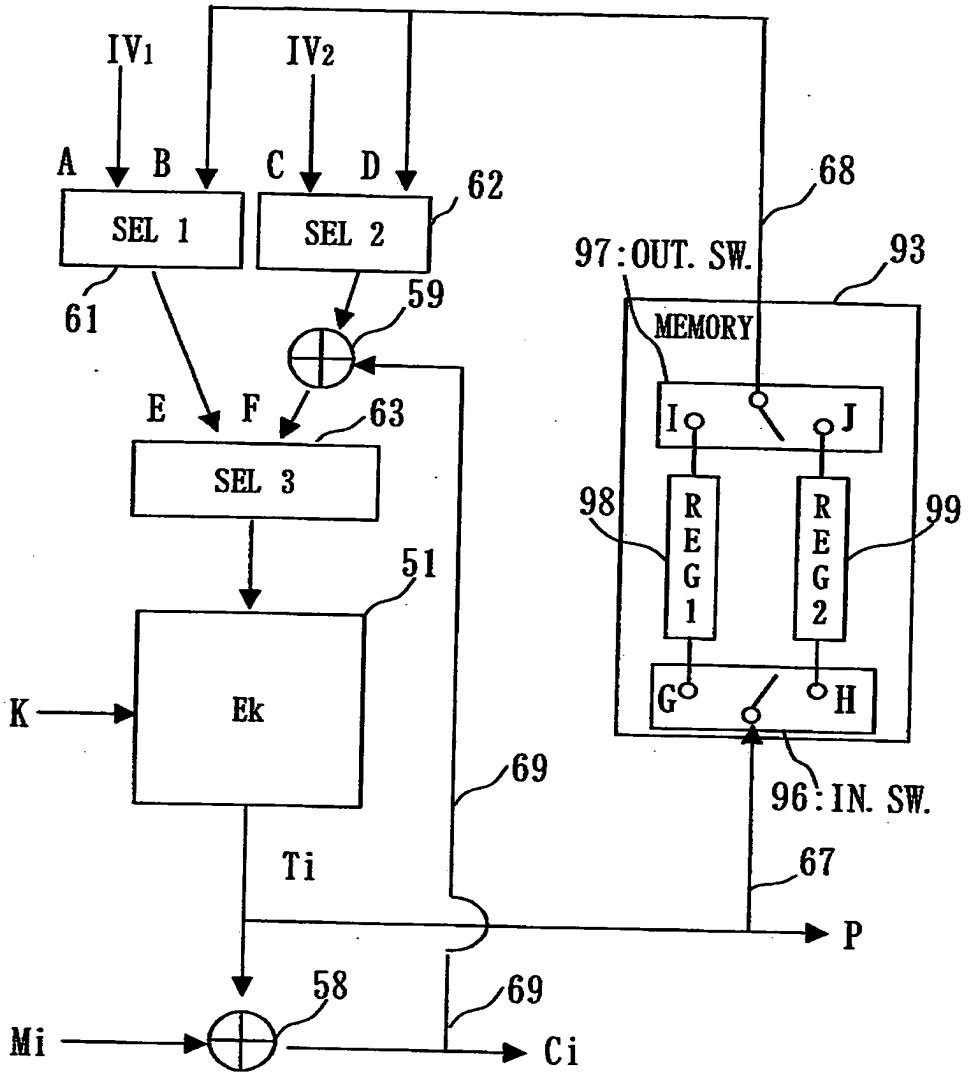
【図２２】


M1
M2
M3
IV1
Ek
Ek
Ek
OBF
C1
C2
C3
IV2
Ek
Ek
Ek
CBC-MAC
P
T
T0
T1
T2
T3
T4

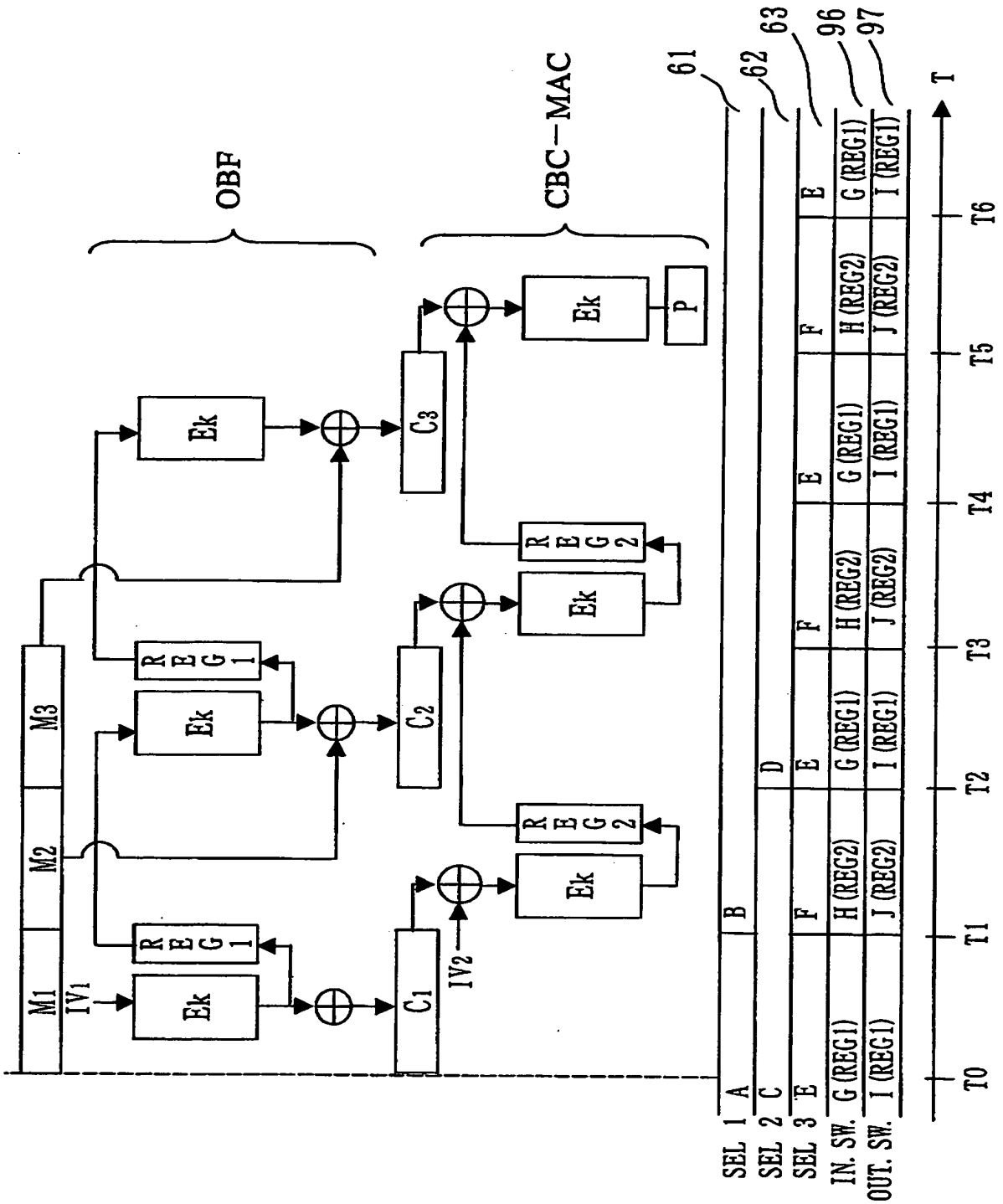
【図２３】


S50
START
S51
i=1
S52
Miを入力して
Miを暗号化して
Ciを生成してCiを出力する
S53
Ciを入力して
Ciを暗号化して
認証子を演算する
S54
i=n
Y
N
S56
認証子付加
END
S55
i=i+1

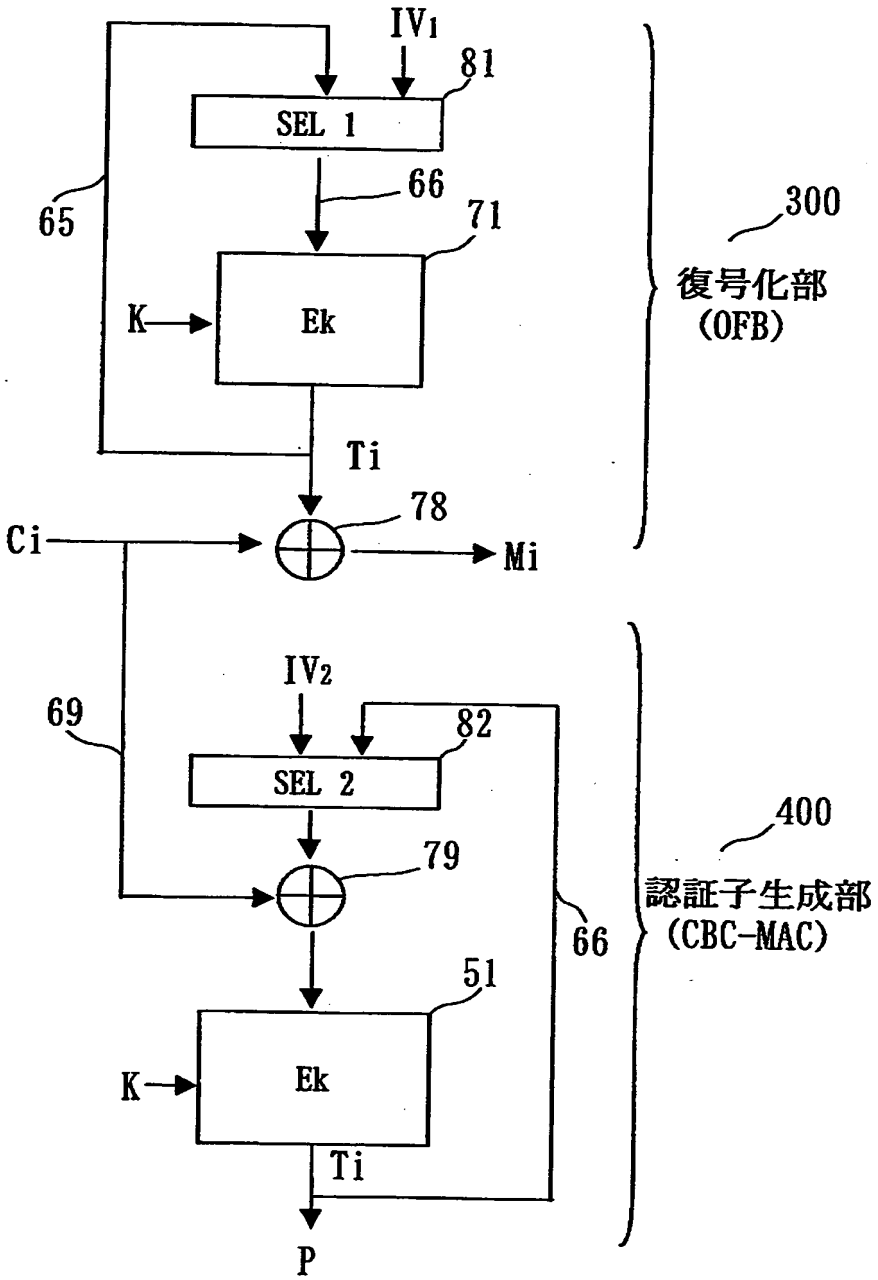
【図２４】


IV1
IV2
A
B
C
D
SEL 1
SEL 2
62
61
59
E
F
63
SEL 3
51
Ek
K
Ti
69
58
Mi
Ci
68
97:OUT. SW.
93
MEMORY
I
J
98
REG1
REG2
99
G
H
96:IN. SW.
67
P

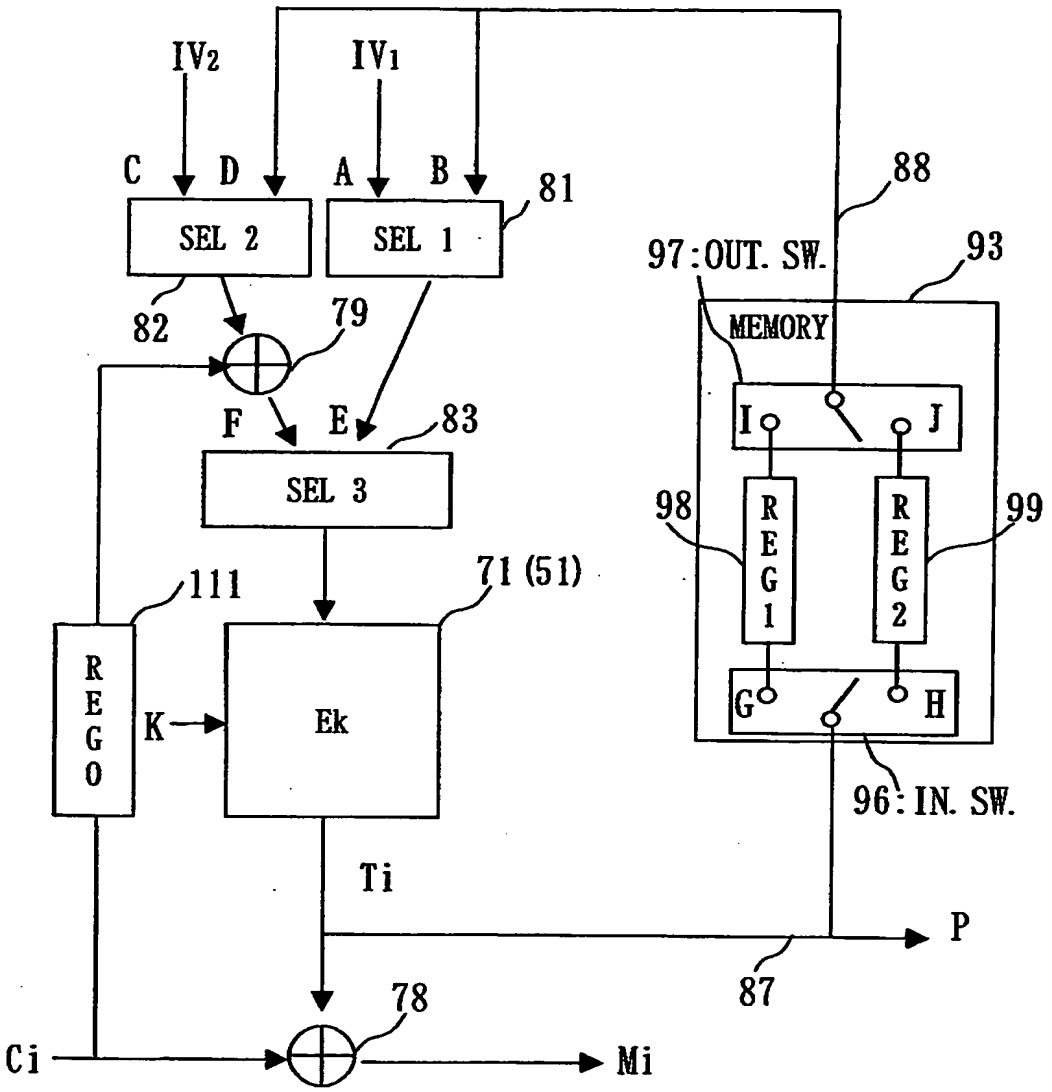
【図２５】


OBF
CBC－MAC
61
62
63
96
97
T
T0
T1
T2
T3
T4
T5
T6
M1
M2
M3
IV1
IV2
Ek
C1
C2
C3
REG1
REG2
P
SEL 1
SEL 2
SEL 3
IN. SW.
OUT. SW.
A
B
C
D
E
F
G (REG1)
H (REG2)
I (REG1)
J (REG2)

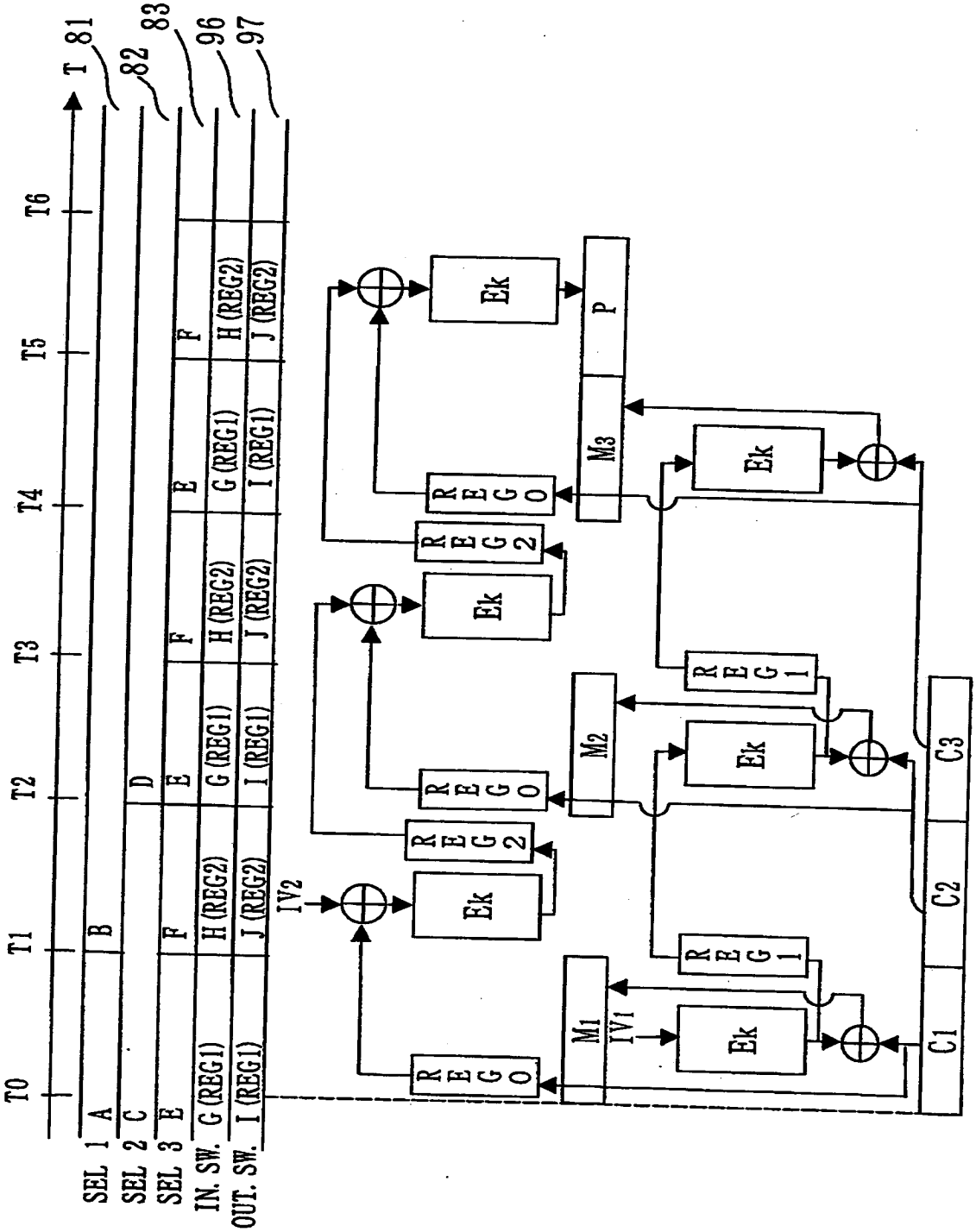
【図２６】


IV1
81
SEL 1
66
65
71
300
K
Ek
復号化部
(OFB)
Ti
78
Ci
Mi
IV2
69
82
SEL 2
400
79
66
認証子生成部
(CBC-MAC)
51
K
Ek
Ti
P

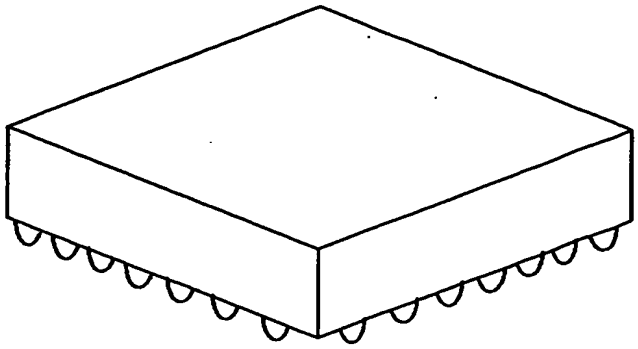
【図２７】


IV2
IV1
C
D
A
B
81
SEL 2
SEL 1
82
79
F
E
83
SEL 3
111
71 (51)
REGO
K
Ek
Ti
Ci
78
Mi
88
97:OUT. SW.
93
MEMORY
I
J
98
REG1
REG2
99
G
H
96:IN. SW.
P
87

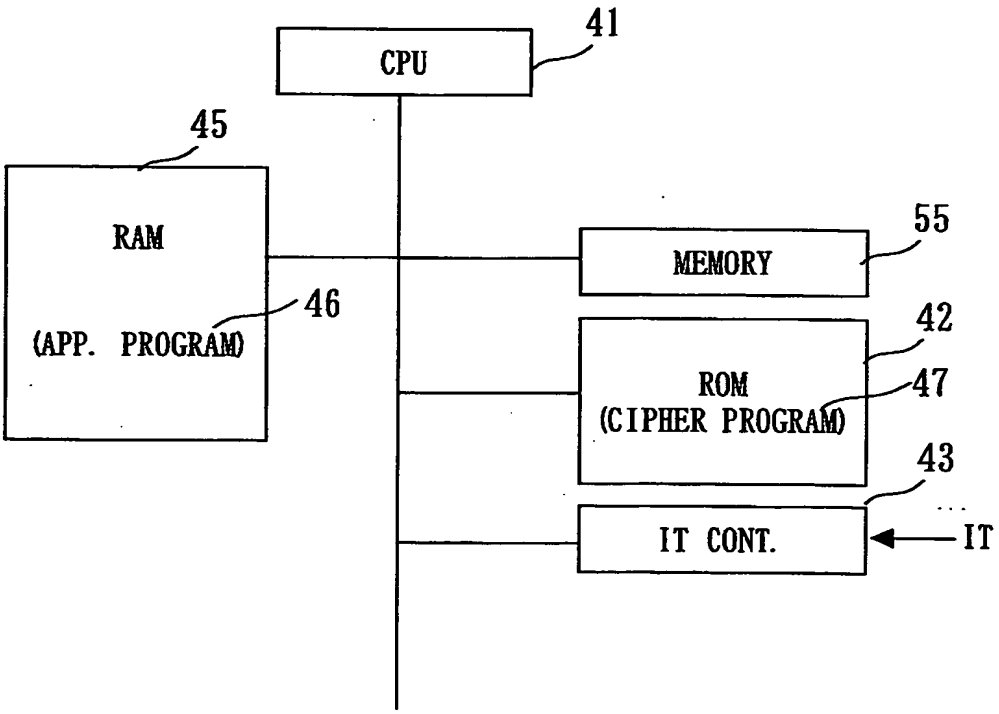
【図２８】


T
81
82
83
96
97
T0
T1
T2
T3
T4
T5
T6
SEL 1
SEL 2
SEL 3
IN. SW.
OUT. SW.
A
B
C
D
E
F
G (REG1)
H (REG2)
I (REG1)
J (REG2)
IV2
IV1
Ek
M1
M2
M3
P
C1
C2
C3
REG 0
REG 1
REG 2

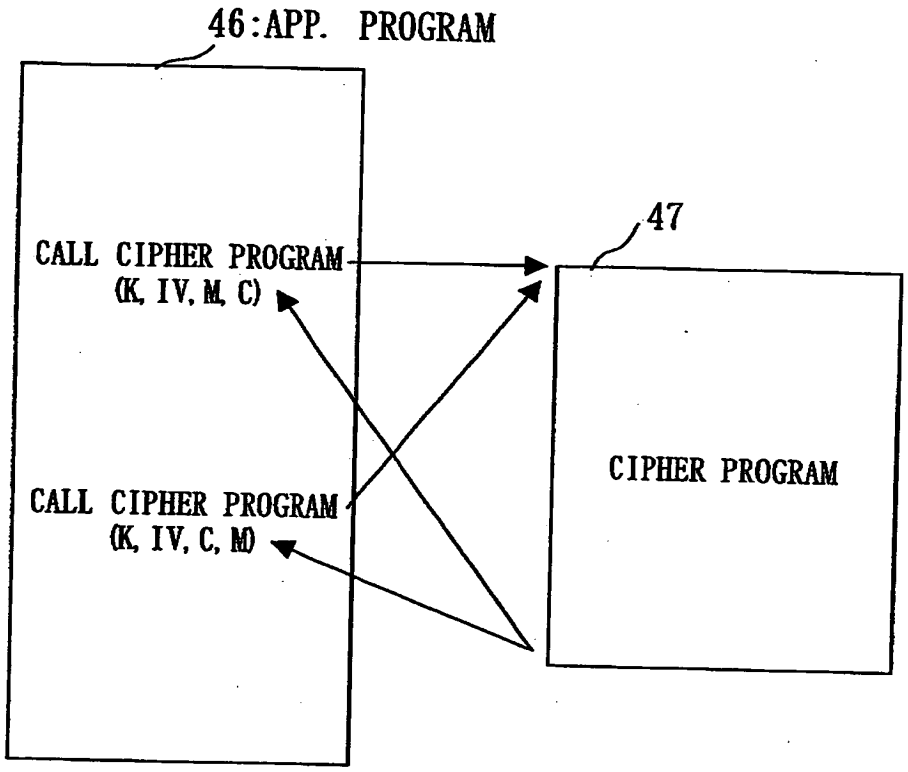
【図２９】



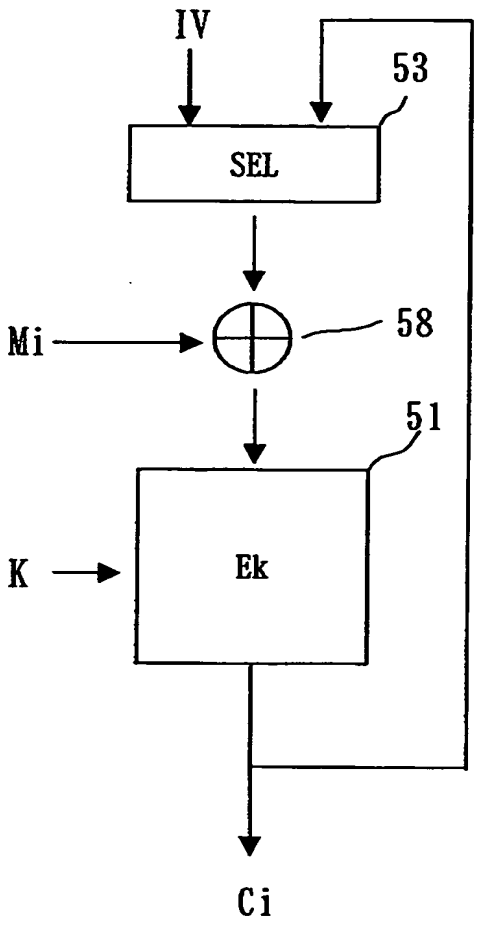
【図３０】


41
CPU
45
RAM
(APP. PROGRAM)
46
55
MEMORY
42
ROM
(CIPHER PROGRAM)
47
43
IT CONT.
IT

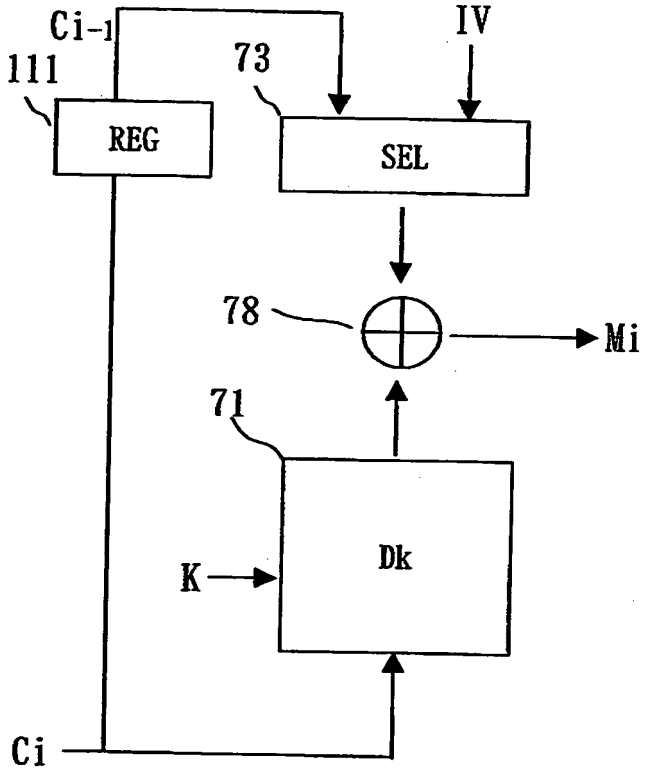
【図３１】


46:APP. PROGRAM
47
CALL CIPHER PROGRAM
(K, IV, M, C)
CALL CIPHER PROGRAM
(K, IV, C, M)
CIPHER PROGRAM

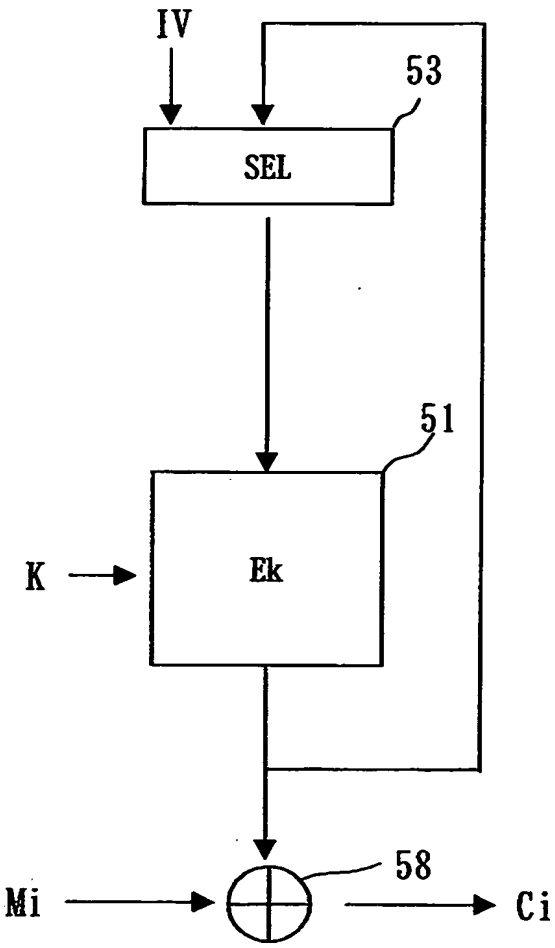
【図３２】



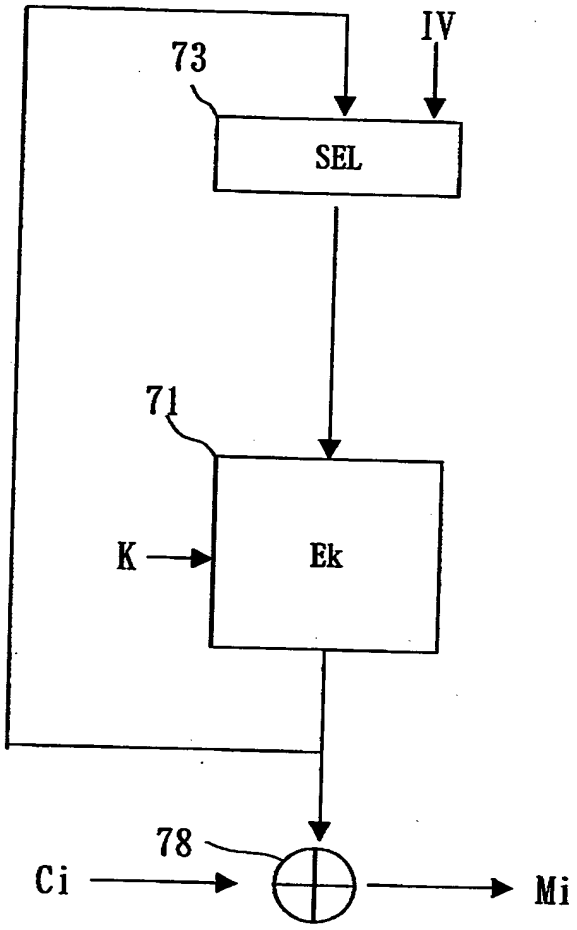
【図３３】



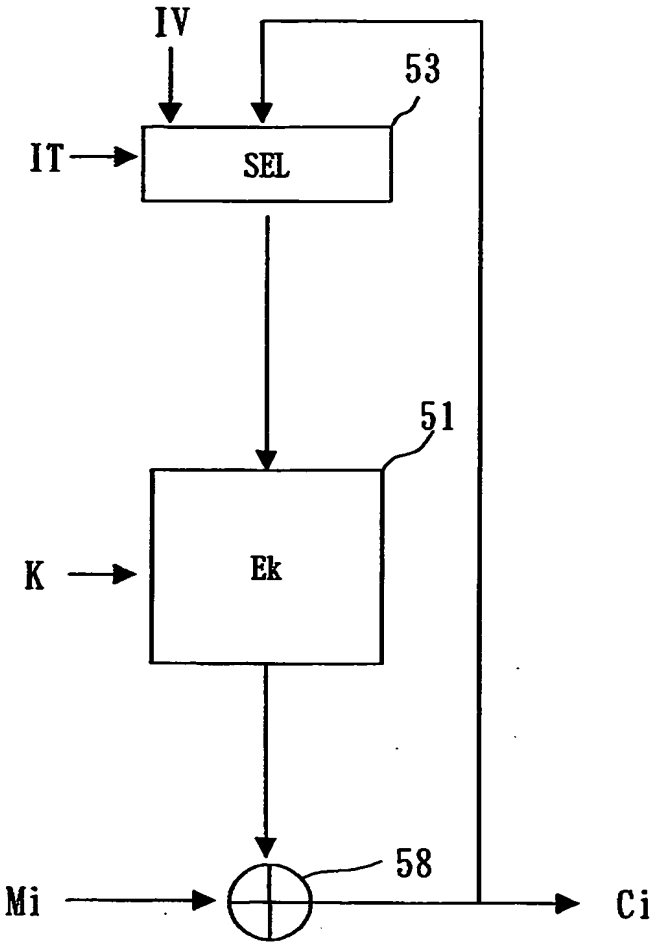
【図３４】



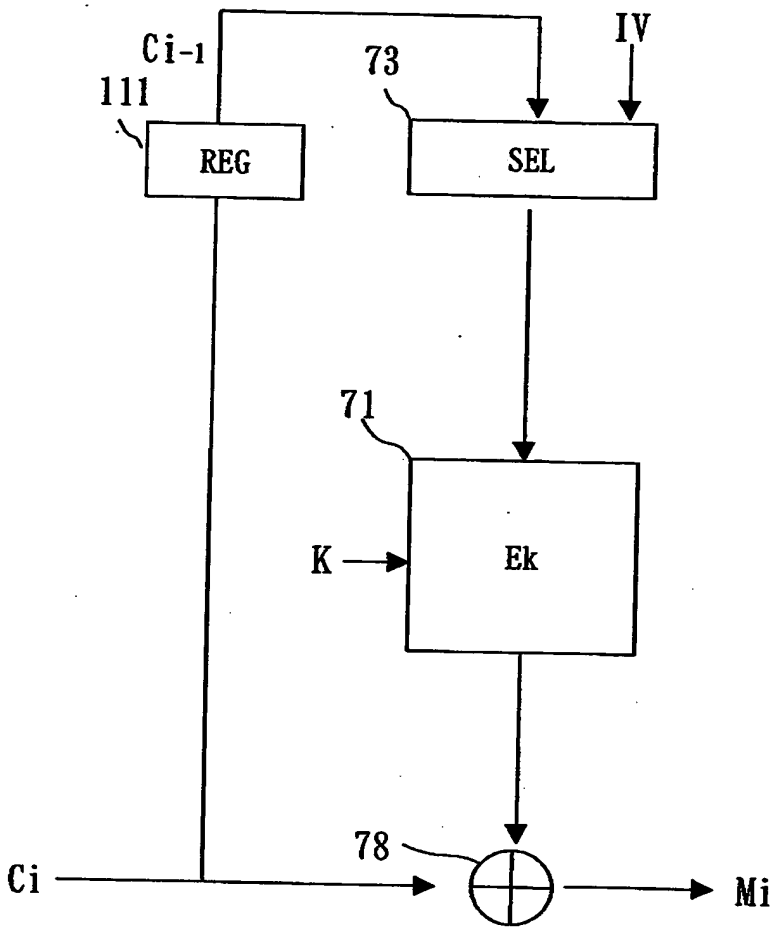
【図３５】



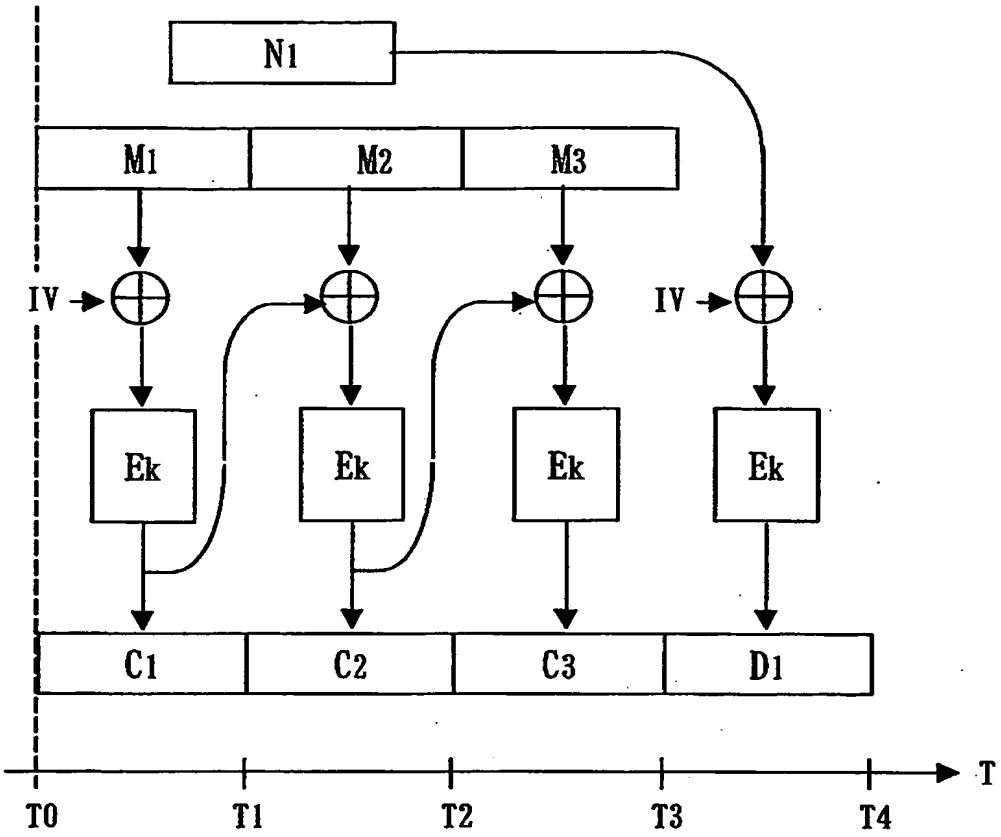
【図３６】



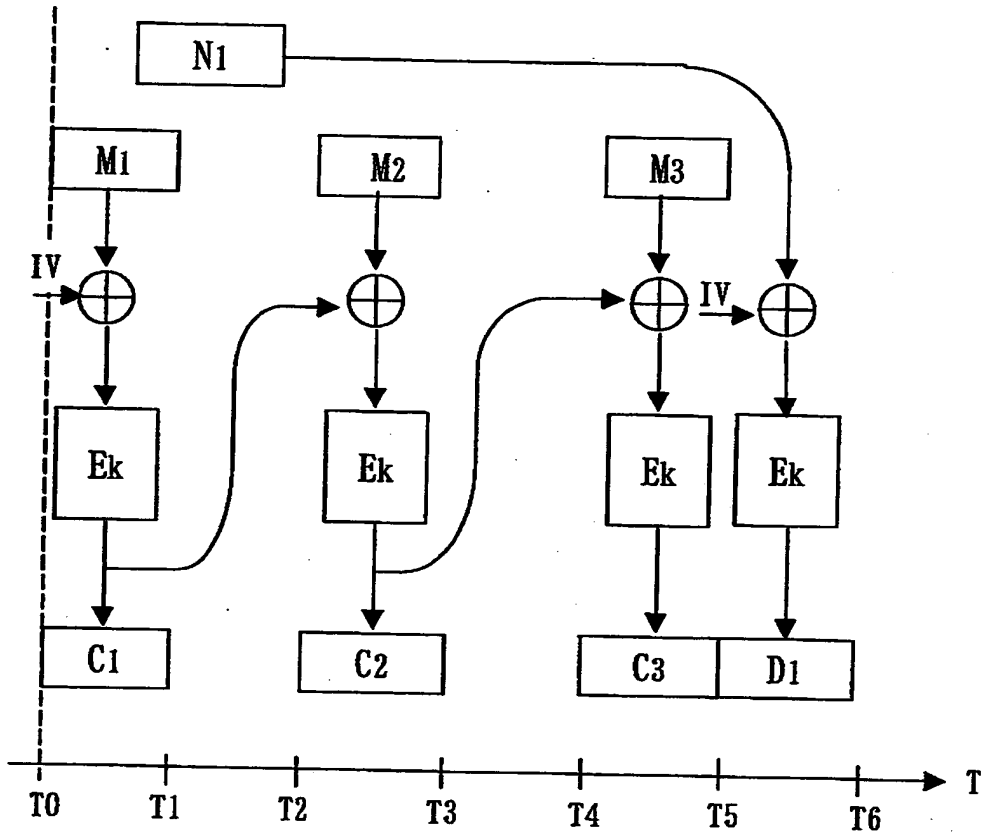
【図３７】



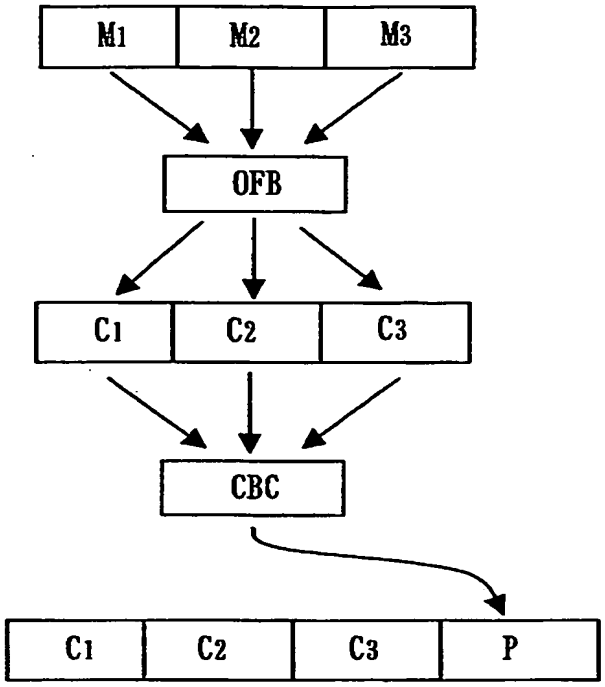
【図３８】



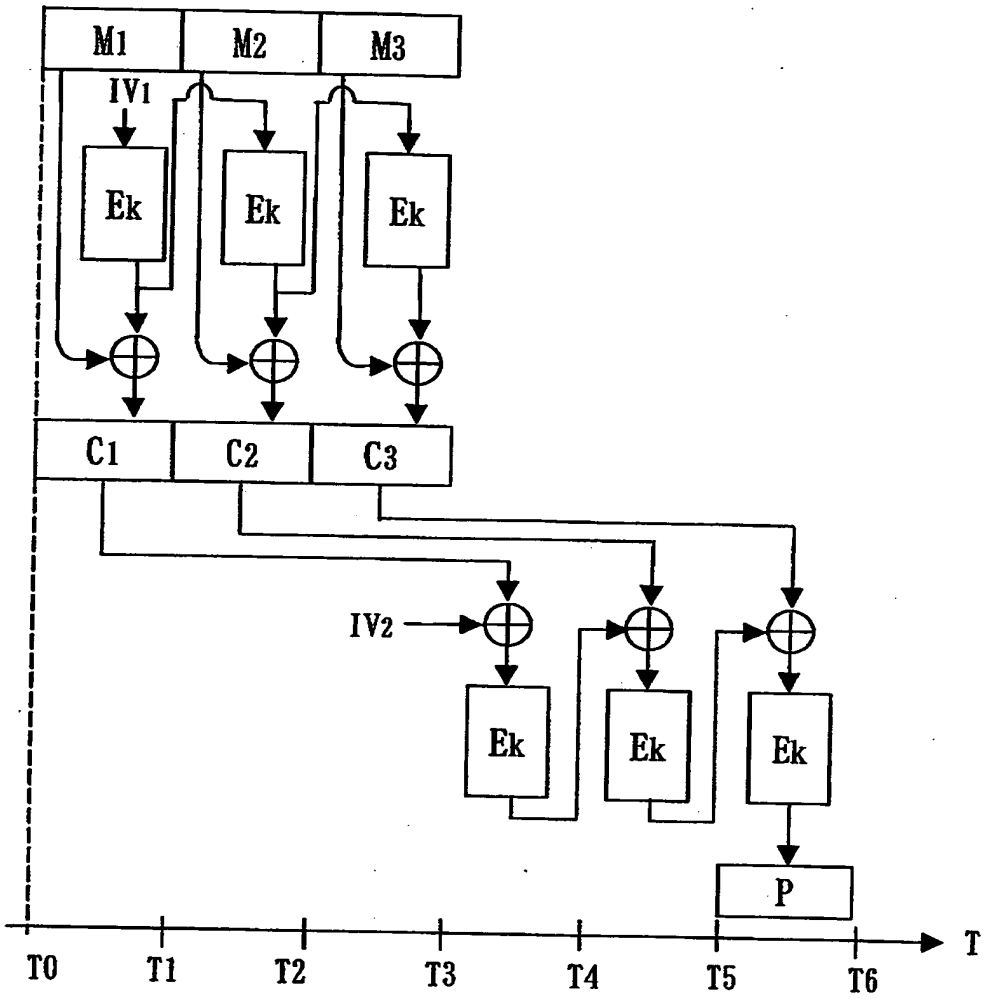
【図３９】



【図４０】



【図４１】



【書類名】　　要約書

【要約】

【課題】　暗号化の最中に他のデータの暗号化を行いたい。

【解決手段】　暗号鍵Ｋを用いた暗号化モジュール５１からセレクタ５４にフィードバックするフィードバックライン６５に対して並列に設けられたメモリ５５を配置する。平文ブロックデータM_iを処理中に他のデータの平文ブロックデータN_iを処理する割り込みＩＴが発生した場合には、割り込みＩＴが発生したときの暗号文ブロックデータC_iをレジスタ５６に記憶させ、平文ブロックデータN_iの処理が終了した時点でメモリ５５に記憶した暗号文ブロックデータC_iをセレクタ５４に選択させることにより平文ブロックデータM_{i+1}の処理を開始する。

【選択図】　　図１

出願人履歴情報

識別番号　〔０００００６０１３〕

１．変更年月日　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都千代田区丸の内２丁目２番３号
氏　名　三菱電機株式会社